3/2022

DVD Deutsche Vereinigung für Datenschutz e.V.

Datenschutz Nachrichten

45. Jahrgang
ISSN 0137-7767
14,00 Euro



Datenschutz und andere Grundrechte

■ Datenschutz als Garant und Ermöglicher von Grundrechten ■ Digitale Grundrechte im internationalen Kontext ■ Digitale Grundrechte im EU-Recht ■ Das Datenschutzgrundrecht – seit 40 Jahren unverzichtbar ■ Das kirchliche Datenschutzrecht ■ Smart Cities ■ Pressemitteilungen ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine



Foto: Pixabay..com

Donnerstag/Freitag, 13./14.10.2022,
Jahreskonferenz,
Forum Privatheit, Berlin

Samstag, 22.10.2022, 10:00 Uhr,
DVD-Vorstandssitzung,
Bonn (Mitglieder, die an der Vorstandssitzung teilnehmen möchten, wenden sich bitte an das DVD-Büro)

Samstag, 22.10.2022,
DVD-Mitgliederversammlung,
Bonn

Mittwoch/Donnerstag, 26./27.10.2022,
Herbstkonferenz, BvD,
Stuttgart

Freitag, 28.10.2022,
Behördentag, BvD,
Stuttgart

Dienstag, 01.11.2022,
Redaktionsschluss DANA 4/2022,
Schwerpunkt: Beschäftigtendatenschutz (geplant)

Mittwoch/Donnerstag, 17./18.11.2022,
46. DAFTA, Datakontext,
Köln/hybrid

Dienstag/Mittwoch, 22./23.11.2022,
3 #Deutschland #Digital #Demokratisch,
Online-Kongress zur digitalen Demokratie

DANA
Datenschutz Nachrichten
ISSN 0137-7767
45. Jahrgang, Heft 3

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftsstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Markus Eßfeld, Riko Pieper, Frank Spaeing
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autorinnen und Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Dr.-Mack-Straße 83
90762 Fürth
www.onlineprinters.de
Tel. +49 (0) 9161 6209800
Fax +49 (0) 9161 8989 2000

Bezugspreis
Einzelheft 14 Euro. Jahresabonnement 48 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Nach einem Jahr kann das Abonnement jederzeit mit einer Frist von einem Monat gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta, Pixabay, iStock, Wikimedia Commons.
Titel: iStock /sdecoret

Editorial

„Der Datenschutz ist zwar kein Supergrundrecht, aber eines, das viele andere Grundrechte erst ermöglicht." So formulierte es Herr Kelber, BfDI, im letzten Jahr auf einer Datenschutzveranstaltung.

Dieser Satz kann als Replik auf die immer wieder vorgetragene Mahnung speziell aus dem Innenministerium verstanden werden (und war wohl auch so gemeint), wonach der Datenschutz kein „Supergrundrecht" sei und somit den ständig erweiterten Befugnissen der Sicherheitsbehörden nicht im Wege stehen darf. Der Punkt ist nur: Von Seiten des Datenschutzes wurde das auch gar nicht behauptet. Trotzdem wird diese Nicht-Aussage immer wieder gern dazu genutzt die Befugnisse der Sicherheits-/Überwachungsdienste kontinuierlich auszuweiten und zwar derart, dass der Datenschutz dabei oft unberücksichtigt bleibt. Ihm kommt dann nur noch eine Feigenblattfunktion zu.

Die Aussage von Herrn Kelber regte die DANA-Redaktion an, das Thema „Datenschutz und andere Grundrechte" zum Schwerpunktthema dieses Heftes zu machen.

Entsprechend haben wir beim BfDI nachgefragt, ob er einen Artikel zu dieser Ausgabe beisteuern und so seine Gedanken aus dem letzten Jahr noch konkretisieren könnte. Er hat sofort zugestimmt. Das Heft beginnen wir folgerichtig mit dem Artikel des BfDI über „Datenschutz als Garant und Ermöglicher von Grundrechten".

Es folgt ein Artikel von Thilo Weichert mit dem Titel „Digitale Grundrechte im internationalen Kontext", der das Thema aus Sicht der deutschen, der europäischen und der internationalen (UN-) Grundrechte ausführlich betrachtet und dabei speziell die Digitalisierung hervorhebt, die bei der Formulierung der Grundrechte zum großen Teil noch nicht berücksichtigt wurde – weil sie damals noch gar nicht berücksichtigt werden konnte.

Achim Klabunde beschreibt das Thema als Mitarbeiter a. D. des Europäischen Datenschutzbeauftragten in einen Artikel aus EU-Sicht, wobei er speziell die historische Entwicklung der EU-Grundrechte darstellt. Frau Leutheusser-Schnarrenberger, Bundes-Justizministerin a. D., erläutert die Entwicklung des Datenschutzes in Deutschland und sieht das Volkszählungsurteil des BVerfG von 1983 als „Zeitenwende". Steffen Pau ergänzt als Leiter der Datenschutzaufsicht für die nordrhein-westfälischen (Erz-)Diözesen, des Verbandes der Diözesen Deutschlands und Leiter des Katholischen Datenschutzzentrums (KdöR) mit einem Beitrag zum Thema: „Das kirchliche Datenschutzrecht". Es folgen zwei Artikel über Smart Cities. Der erste von Heinz Alenfelder über „Die Entwicklung einer Smart City – Im Fokus: Bürgerbeteiligung" und der zweite von Astrid Donaubauer-Grobner über „Smart Cities und Datenschutz". Ein Artikel von Frau Yu Du (Partnerin MMLC Group Lawyers & Consultants) mit dem Titel: „China's First Face Recognition Case Study", den wir im englischen Original (sowie in einer durch uns – unterstützt durch deepl.com – erstellten deutschen Übersetzung) wiedergeben, schließt das Schwerpunktthema ab.

Wie immer gibt es auch in diesem Heft weitere Beiträge, die nicht explizit zum Schwerpunktthema geschrieben wurden, die aber auf den zweiten Blick trotzdem dazu passen:

Riko Pieper hat in seiner Eigenschaft als Sprecher des Arbeitskreises Kryptografie (AK-Krypto) des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. einen Artikel über Impfzertifikate im BvD-Blog veröffentlicht, den wir gerne auch in diesem Heft abdrucken. Ein relativ neues Thema ist der „Matrixcode", den man seit kurzer Zeit auf Briefmarken sehen kann. Heinz Alenfelder hat dazu recherchiert und zusammengetragen, welche Daten dabei von wem verarbeitet werden und wer welche dieser Informationen abrufen kann.

Danach sind noch ein „Offener Brief anlässlich der Frühjahrskonferenz der Innenminister und -senatoren" gegen die Vorratsdatenspeicherung, der von der DVD mitunterzeichnet wurde, sowie eine aktuelle Presseerklärung der DVD zur Plattform „handelsregister.de" abgedruckt und es folgen die aktuellen Nachrichten, Urteile und Buchbesprechungen. Dabei fällt auf, dass die Nachrichten, die wie immer unabhängig vom Schwerpunktthema zusammengestellt wurden, erstaunlich oft neben dem Datenschutz auch eines der Grundrechte bzw. eine mögliche Beeinträchtigung eben dieser thematisieren. Oder, um es mit den Worten eines ehemaligen deutschen Innenministers zusammenzufassen: Einige der Beiträge in diesem Heft könnten Sie beunruhigen.

Viel Spaß beim Lesen wünscht die DANA-Redaktion.

Autorinnen und Autoren dieser Ausgabe:

Prof. Ulrich Kelber
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI), www.bfdi.de

Dirk Müllmann
Rechtsreferendar beim BfDI, www.bfdi.de

Dr. Thilo Weichert
Vorstandsmitglied in der DVD, Netzwerk Datenschutzexpertise, weichert@datenschutzverein.de

Achim Klabunde
Mitarbeiter a. D. des Europäischen Datenschutzbeauftragten

Sabine Leutheusser-Schnarrenberger
Bundesministerin der Justiz a. D.

Steffen Pau
leitet die Datenschutzaufsicht für die nordrhein-westfälischen (Erz-)Diözesen und den Verband der Diözesen Deutschlands; Leiter des Katholischen Datenschutzzentrums (KdöR), www.katholisches-datenschutzzentrum.de

Heinz Alenfelder
Vorstandsmitglied in der DVD, alenfelder@datenschutzverein.de

Astrid Donaubauer-Grobner
Risikomanagerin, astrid@donaubauer-grobner.at

Yu Du
Partnerin MMLC Group Lawyers & Consultants, yudu@mmlcgroup.com

Riko Pieper
Vorstandsmitglied in der DVD, pieper@datenschutzverein.de

Ulrich Kelber, Dirk Müllmann

Datenschutz als Garant und Ermöglicher von Grundrechten

Die Liste der Dinge, von denen behauptet wird, dass der Datenschutz sie verhindere, ist lang: Mal ist er dafür verantwortlich, dass während der Corona-Pandemie keine effiziente Kontaktnachverfolgung per App stattfinden oder kein Impfregister eingerichtet werden kann, dann soll er die effektive Arbeit der Sicherheitsbehörden behindern und Täter schützen und ganz generell behindere er die Digitalisierung und den Fortschritt in Deutschland. Die sachliche und fachliche Wahrheit steht dabei aber auf einem ganz anderen Blatt. Unser Datenschutz ist europäisch. Dass Deutschlands Probleme mit der Digitalisierung also gerade auf ihn zurückzuführen sein sollen, ist verwunderlich, da der Großteil unserer europäischen Partner diese Probleme nicht zu haben scheint. Dass die Rechtsprechung den Einsatz von Techniken und Instrumenten insbesondere deshalb für verfassungswidrig hält, weil der deutsche Gesetzgeber sie zu exzessiv ausgestaltet und zu pauschal einsetzt, wird nicht erwähnt. Und, dass der Datenschutz während der Corona-Pandemie keine Maßnahme verhindert hat, die deutsche Corona-App 45 Millionen Mal heruntergeladen wurde und Impfregister in Österreich, Schweden, Finnland und den Niederlanden existieren, in denen dieselben datenschutzrechtlichen Grundsätze gelten wie in Deutschland, bleibt unbeachtet.

Selbst wenn sich viele Kritikpunkte am Datenschutz als offensichtlich unbegründet erweisen und man dazu neigt sie zu ignorieren, hat ein solches, von der Tatsachenlage entkoppeltes, Narrativ in Bezug auf den Datenschutz dennoch gesellschaftliche Konsequenzen. Es etabliert eine Grundeinstellung bei den Bürgerinnen und Bürgern, nämlich: Datenschutz sei ein großer Verhinderer. Gepaart mit fehlendem Wissen über die Macht der Daten und über die Analysemöglichkeiten moderner Techniken in einer umfassend vernetzten Gesellschaft reduziert das die Wahrnehmung des Datenschutzes innerhalb der Gesellschaft auf banale und oftmals negative Berührungspunkte, wie das Wegklicken eines nervigen Cookie-Banners vor einem Webseitenbesuch.

Tatsächlich ist Datenschutz aber ein Ermöglicher. Er erfüllt nicht nur eine eigenständige Funktion bei der Wahrung der Privatheit und Selbstbestimmung der Bürgerinnen und Bürger, sondern schützt auch die Ausübung anderer Grundrechte und überführt sie von einer analogen in eine digitale Gesellschaft. Er hat damit eine Schlüssel- und Garantenfunktion zur Wahrung der Ausübung aller anderen Grundrechte. Diese Rolle des Datenschutzes für die Grundrechtsausübung sowie die demokratische Gesellschaft verdient es deutlicher beleuchtet zu werden.

Schutz vor „Chilling Effects"

Die unterstützende, manchmal sogar dienende Funktion des Datenschutzes für die Ausübung anderer Grundrechte des Grundgesetzes (GG) ist schon in seiner Geburtsstunde betont worden. Nicht umsonst argumentierte das Bundesverfassungsgericht in seinem Volkszählungsurteil, dass die Ausübung der eigenen Freiheitsrechte wesentlich davon abhänge das Wissen des Gegenübers abschätzen zu können und nicht damit rechnen zu müssen, dass abweichendes Verhalten wahrgenommen, gespeichert und gegen einen verwendet werde. Denn, *„[w]er damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten."*

Solche Auswirkungen auf die Unbefangenheit des Grundrechtsgebrauchs sind vom Verfassungsgericht in der Folge in unterschiedlichen, auch nicht datenschutzrechtlichen Kontexten identifiziert und als hemmende, einschüchternde oder abschreckende Wirkung bezeichnet worden. Dem Vorbild des Europäischen Gerichtshofs für Menschenrechte (EGMR) folgend, hat sich für sie in der Wissenschaft der Begriff der *„Chilling Effects"* etabliert. Auch, wenn selbst der EGMR den Begriff nicht vollständig einheitlich verwendet, bezeichnen Chilling Effects in erster Linie den Versuch des Staates oder seiner Bevollmächtigten ein Klima der Selbstzensur zu schaffen, unabhängig davon, ob das in Betracht gezogene Verhalten durch das Recht geschützt wird. Chilling Effects können sich im Kontext eines jeden Grundrechts auswirken. Gerade im Zusammenhang mit der Meinungs-, Presse- und Versammlungsfreiheit kommt ihnen jedoch besondere Bedeutung zu. Eine der Hauptquellen von Chilling Effects stellen dabei staatliche Überwachungsmaßnahmen dar, wie auch die Etablierung einer Überwachungsgesamtschau als Prüfungsmaßstab des Bundesverfassungsgerichts für neue gesetzgeberische Maßnahmen im Sicherheitsrecht verdeutlicht. Zugleich wirken sich Einschüchterungseffekte damit aber auch gerade in einem Bereich aus, in dem ihnen durch die konsequente Anwendung des Grundrechts auf informationelle Selbstbestimmung umfassend begegnet werden kann. Effektivem Datenschutz kommt so eine Funktion als Mittel gegen Chilling Effects zu, indem er ein Schutzniveau gegen staatliche Kontrolle garantiert, das jeder einzelnen Person eine angstfreie und ungestörte Ausübung grundrechtlich geschützter Tätigkeiten ermöglicht.

Kritiker wenden gegen dieses Abschreckungsargument oft ein, dass die Grundrechtsausübung in einer gefestigten Demokratie wie der Deutschlands gewährleistet und angesichts einer etablierten rechtsstaatlichen

Ordnung auch zukünftig nicht gefährdet sei. Es handle sich also um eine eingebildete und keine reale Gefahr. Doch belegen verschiedene aktuelle Beispiele, dass auch etablierte Demokratien sich autoritär entwickeln und gesellschaftliche Rollbacks vollziehen können. Zudem zeigt die Beschreibung der Chilling Effects doch gerade, dass es der tatsächlichen Errichtung eines undemokratischen Überwachungsstaates und rechtlich fixierter Konsequenzen für eine Selbstbegrenzung der Bürgerinnen und Bürger bei der Grundrechtsausübung gar nicht bedarf. Dies lässt sich auch anhand eines Beispiels zur Selbstreflektion gut nachvollziehen: Wie fühlt sich der Gedanke an, dass der Staat, zum Beispiel aus Gründen des Jugendschutzes, Messengernachrichten anlasslos mitlesen kann? Würde man unter solchen Umständen gegenüber seinen engsten Freunden oder seiner Familie noch seine privatesten Gedanken im Chat mitteilen? Selbst wenn man wüsste, dass ein Eingreifen des Staates gesetzlich nur in den oben genannten Fällen möglich wäre, würde man erwarten, dass er sich an diese Begrenzung hält? Oder hat der Staat zu oft gezeigt, dass das Vorhandensein von Informationen zu einem Zweck immer auch die Begehrlichkeit in Bezug auf ihre Verwendung in anderen Kontexten erzeugt?

Für die meisten Menschen genügt der bloße Gedanke, dass kritisches oder abweichendes Verhalten wahrgenommen und gegen sie verwendet werden könnte, um eine selbstauferlegte Zurückhaltung bei der Ausübung grundrechtlich geschützter Tätigkeiten fest zu verankern. In anderen Worten: Ein Schaden für den Einzelnen und damit auch die Gesellschaft – hierzu in der Folge – wird abseits der eigentlichen Zielrichtung einer sicherheitsrechtlichen Maßnahme angerichtet, lange bevor aus ihr überhaupt Konsequenzen erwachsen sollen. Dem vermag Datenschutz vorzubeugen.

Gewährleistung von demokratischen und pluralistischen Strukturen

Vor dem Hintergrund dieser Überlegung endet die Gewährleistungs- und Unterstützungsfunktion für andere Grundrechte durch das Grundrecht auf informationelle Selbstbestimmung nicht bei den Art. 1 bis 19 GG. Ihm kommt vielmehr auch eine wesentliche Rolle bei der Garantie der demokratischen Grundordnung und der Pluralität der Gesellschaft zu, die selbst wiederum Grundvoraussetzungen für eine effektive Grundrechtswahrnehmung darstellen. Auch dies hat das Bundesverfassungsgericht in Bezug auf das Grundrecht für informationelle Selbstbestimmung schon früh erkannt, indem es auf die Rückkopplung individueller Entfaltungschancen an die Funktionsfähigkeit des Gemeinwesens verwiesen hat, die selbst wiederum wesentlich von der Handlungs- und Mitwirkungsfähigkeit der Bürgerinnen und Bürger und somit deren Selbstbestimmung abhängt. So erfüllt funktionierender Datenschutz auch eine unersetzliche Aufgabe für die Mitwirkung der*s Einzelnen in der demokratischen Gesellschaft.

Die Erfahrung der letzten Jahre zeigt zudem, dass datenschutzrechtliche Gewährleistungen auch als Garanten für die Unabhängigkeit und Diversität von Meinungsbildungsprozessen in der Demokratie einstehen müssen. Populistische Erfolge der jüngeren Vergangenheit sind eng mit dem Missbrauch von Datenmacht verknüpft. Der Brexit oder auch die Wahl Donald Trumps zum amerikanischen Präsidenten wurden entscheidend durch die umfassenden Auswertungen von Nutzerdaten, die Erstellung von Nutzerprofilen und den Einsatz von hochindividualisierten Social-Media-Kampagnen vorangetrieben. Mithilfe von Methoden wie Microtargeting oder Geofencing werden so mittels Datenauswertung Echokammern geschaffen, die den kritischen Diskurs ersticken, den jede demokratische Gesellschaft benötigt. Ein Aufeinandertreffen und ein konstruktiver Austausch verschiedener Ansichten finden so nicht mehr statt. Vielmehr wird der Trend zum Extremen gefördert und mit Sichtbarkeit und Klicks belohnt.

Diese Techniken nehmen dabei zugleich großen Einfluss auf die Freiheit unserer Entscheidungen. Indem sie steuern, was uns in der Timeline eines sozialen Netzwerks angezeigt wird, regeln sie, zu welchen Informationen wir bequemen Zugang haben und was wir somit regelmäßig zur Grundlage unserer Entscheidungen, Einstellungen und Ansichten machen. Mit ihrer Hilfe fällt es leicht Nutzer in einem bestimmten Sinne zu beeinflussen bzw. sie für oder gegen eine Sache einzunehmen. Noch bedenklicher wird dieses Vorgehen dadurch, dass es vorgaukelt, Nutzer träfen eine eigene, freie und gar informierte Entscheidung auf der Basis selbstgewählter Informationen. Tatsächlich verkommt die Freiheit der Entscheidung vor dem Hintergrund dieser Techniken jedoch vielmehr zu einer reinen Illusion. Hier liegt in der Zukunft eine Herkulesaufgabe für den Datenschutz, bei der er seine Rolle als Garant für die Entfaltungsmöglichkeit anderer Grundrechte noch viel ernster nehmen muss. Bei der Regulation der Erstellung und Verwendung umfassender Nutzerprofile kann der Datenschutz seine Gewährleistungsfunktion für das Funktionieren des gesellschaftlichen Diskurses voll ausschöpfen und so seiner Rolle als Ermöglicher nachkommen.

Dies zeigt: Datenschutz schützt nicht die Daten sondern die Menschen. Er schützt vor Manipulation und verschleierter Fremdbestimmung. Er ist daher selbst nicht nur die regulatorische Verkörperung informationeller Selbstbestimmung, sondern er sichert und ermöglicht allen Menschen darüber hinaus generell die allgemeine Selbstbestimmung des eigenen Lebens schlechthin.

Datenschutz zwischen Privaten

Am Beispiel der sozialen Medien offenbart sich auch die Bedeutung der Grundrechtswahrnehmung im Verhältnis zu anderen Privaten. Der Marktplatz einer Stadt hat als Ort für den Austausch von Meinungen und Informationen eklatant an Bedeutung verloren. Die Funktion, die dieser Institution des Forums in Bezug auf die Grundrechtsbetätigung zukam, erfüllen nunmehr Onlineplattformen, auf denen Begegnung und gerade auch Meinungsäußerungen und -austausch stattfinden. Daher wächst die Bedeutung der ebenfalls für den

Staat aus dem Recht auf informationelle Selbstbestimmung erwachsenden Schutzpflichten, mit denen der Datenschutz mittelbar in das Verhältnis zwischen Privaten hineinwirkt. Je stärker die Möglichkeit der effektiven Wahrnehmung von Grundrechten bzw. grundrechtlich geschützten Tätigkeiten von Dritten abhängt, desto wichtiger sind gute datenschutzrechtliche Regelungen und deren konsequenter Vollzug gerade auch in diesen Verhältnissen.

Gewährleistung von Gleichheitsrechten und Teilhabe

Datenschutz kommt aber nicht nur die Rolle der Abwehr von Einflussnahme bei der Wahrnehmung anderer Grundrechte zu. Vielmehr hat er auch bei der Durchsetzung des Gleichheitsgrundrechts aus Art. 3 Abs. 1 GG erhebliche Bedeutung. So kann Ungleichbehandlung insbesondere dadurch verhindert werden, dass für eine Diskriminierung nutzbare Merkmale gar nicht erst erhoben werden können. Hierbei kommt der Grundsatz der Datenminimierung zum Tragen, aus dem sich die Voraussetzung der Erforderlichkeit einer Datenverarbeitung ableiten lässt. Erst kürzlich hat die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen eine Geldbuße gegen eine Wohnungsbaugesellschaft verhängt, die Daten zu den Frisuren, dem Körpergeruch und dem Auftreten von Mietinteressenten und somit zu Informationen gespeichert hat, die für die Eingehung eines Mietverhältnisses nicht erforderlich sind, die gleichzeitig aber für eine diskriminierende Auswahlentscheidung bei der Wohnungsvergabe herangezogen werden können. Gerade für Menschen, die zu diskriminierten gesellschaftlichen Gruppen gehören, erfüllt Datenschutz somit eine wesentliche Funktion bei der Wahrnehmung ihrer Rechte auf Teilhabe und der Erfüllung elementarer Grundbedürfnisse wie Arbeit oder Wohnen.

Die Schutz- und Gewährleistungsmöglichkeiten des Datenschutzes erschöpfen sich zugleich nicht in der Verhinderung einer Verarbeitung nicht erforderlicher und potenziell diskriminierender Merkmale. Datenschutz zielt vielmehr auch auf die Qualität von Informationen als Entscheidungsgrundlage, indem er fordert, dass verarbeitete Daten richtig und erforderlichenfalls auf dem neusten Stand sind sowie dass unrichtige Daten gelöscht oder berichtigt werden. Dies hat nicht nur Bedeutung für den Einzelnen, sondern auch eine gesamtgesellschaftliche Dimension. Indem Datenschutz ein Schlaglicht auf den Aspekt der Datenqualität wirft, macht er auch auf das Problem aufmerksam, dass Datengrundlagen, die diskriminierende gesellschaftliche Zustände abbilden, sich nicht als Grundlage für Prognosen und Entscheidungen eignen, da andernfalls eine Perpetuierung der in ihnen abgebildeten Ungleichbehandlung zu befürchten steht.

Datenschutz ermöglicht die Grundrechtsausübung

Anders als oftmals behauptet, ist Datenschutz nicht der große Verhinderer. Seine Rolle bei der Wahrnehmung anderer Grundrechte erstreckt sich sowohl auf die Beseitigung etwaiger Einschüchterungen durch Chilling Effects als auch die Gewährleistung von Umständen, die eine unbeeinflusste demokratische Teilhabe jeder Person ermöglichen, sowie die Unterstützung bei diskriminierungsfreier gleichberechtigter Teilhabe an der Gesellschaft. Dabei ist Datenschutz aber nicht paternalistisch. Er stellt, zum Beispiel in Form der Betroffenenrechte, Instrumente bereit, die uns alle zur selbstständigen Durchsetzung des Rechts auf informationelle Selbstbestimmung und damit verbunden auch anderer Grundrechte ermächtigen. So übergibt er aber auch jeder einzelnen Person eine Verantwortung für die eigene Grundrechtswahrnehmung, die in der Frage kumuliert: Wie ernst will ich Datenschutz nehmen? Hierauf müssen Bürgerinnen und Bürger nicht nur selbst eine abstrakte Antwort finden, sondern gegebenenfalls auch konkret danach handeln, um eigenes Verhalten datenschutzfreundlich auszurichten. Für den Staat und Unternehmen erwächst daraus jedoch auch die Verantwortung Digitalisierung gut umzusetzen. Sie können und dürfen nicht darauf vertrauen oder gar fordern, dass die Bürgerinnen und Bürger schlecht umgesetzte technische Maßnahmen durch den Verzicht auf ihre Rechte legitimieren. Wer erreichen will, dass Digitalisierung Neues ermöglicht, muss Datenschutz zuvor als Ermöglicher für eine demokratische und digitale Gesellschaft erkennen, damit sich bisher unentdeckte Möglichkeiten der Digitalisierung eröffnen.

Thilo Weichert

Digitale Grundrechte im internationalen Kontext

Angesichts des Kriegs in der Ukraine ist von einer „Zeitenwende" die Rede. Die Position der westlichen Welt gegenüber Russland und auch China steht auf dem Prüfstand. Das bisherige westliche Credo „Wandel durch Handel" hat ausgedient. Die westliche Werteorientierung mit der Betonung demokratischer Entscheidungsfindung und der rechtsstaatlich abgesicherten Gewährleistung der Menschenrechte spielen plötzlich im globalen Diskurs eine Rolle, wo bisher nur von der Globalisierung der Märkte die Rede war. Durch die Aufkündigung einer auf Regeln beruhenden Weltordnung durch den russischen Präsidenten Wladimir Putin besinnt sich die westliche Welt auf die Regulierung dieser Weltordnung.

Die „Zeitenwende" äußert sich praktisch zunächst in einer Aufwertung des Militärs, nicht aber gerade auch der Grundrechte. Dessen ungeachtet haben Grundrechte eine neue Relevanz gewonnen. Der Schutz der Bürgerrechte wird zumindest indirekt wieder als das erkannt, was er ist: die Voraussetzung für eine freiheitliche und friedliche zivilisierte Welt. Dabei spielen auch informationelle Grundrechte eine Rolle, wenn etwa die Überwachungsstaatlichkeit in Xinjiang zum Argument dafür wird eine staatliche Investitionsgarantie für das dortige ökonomische VW-Engagement zu verweigern.[1]

Die „Zeitenwende" ist ein guter Grund, eine Positionsbestimmung informationeller Grundrechte vorzunehmen und deren globale Relevanz zu hinterfragen. Dabei spielt das Grundrecht auf Datenschutz eine zentrale Rolle, zumal es sich als Antwort auf die Polizeistaatlichkeit Russlands und Chinas eignet. Es geht darum den instrumentellen Charakter der Grundrechte in der globalen Politik einerseits zu erkennen und andererseits zugleich diese Erkenntnis zu nutzen, um die digitalen Grundrechte zu stärken.

1. Die Entwicklung der digitalen Grundrechte aus dem Datenschutz

Datenschutz ist die Mutter und der Ausgangspunkt digitaler Grundrechte. Bevor sich der Datenschutz in den 70er-Jahren in Deutschland und Europa entwickelte, wurden Grundrechte analog und materiell gedacht und normiert. Dies gilt für die englische Magna Charta von 1215, für die US-amerikanische Bill of Rights von 1789, für die französische Erklärung der Menschen- und Bürgerrechte von 1789 bis hin zur allgemeinen Erklärung der Menschenrechte der Vereinten Nationen von 1948. Das gilt auch in Deutschland für den Grundrechtsschutz in den Art. 114 ff. der Weimarer Reichsverfassung[2] und dann für den prominent platzierten Grundrechtskatalog im Grundgesetz (GG) der Bundesrepublik Deutschland von 1949.

Die Anpassung des Grundrechtsschutzes an die neue Realität der Automatisierung bzw. Informatisierung erfolgte ausgehend von Deutschland mit dem Volkszählungsurteil des Bundesverfassungsgerichts (BVerfG) 1983.[3] Soweit völkerrechtliche Ansätze verfolgt wurden, etwa mit der Datenschutzkonvention des Europarats von 1981[4] oder den OECD-Leitlinien von 1980[5], wurde dies vorrangig mit dem Ziel der Erleichterung des internationalen Datenverkehrs begründet, dem individuelle Schutzerwägungen entgegen stehen können. Diese Erwägungen werden so zur Blaupause: Internationalen Austausch – auch wissenschaftlich oder ökonomisch motiviert – sollte und darf es nur geben, wenn nachweisbar bürgerrechtliche Mindeststandards eingehalten werden.

Nicht dem Abbau ökonomischer Hindernisse, sondern vorrangig dem Ziel des humanitären Schutzes dienen die „Richtlinien zur Verarbeitung personenbezogener Daten" durch einen Unterausschuss für die „Verhütung von Diskriminierungen sowie den Schutz von Minderheiten, die Menschenrechte und die wissenschaftlich-technische Entwicklung" der UN-Menschenrechtskommission von 1985, die ebenso wie bisher fast sämtliche völkerrechtlichen Normen nicht bindend sind.[6] Eine höhere Verbindlichkeit kommt der Europäischen Menschenrechtskonvention von 1950 zu, die über den Geltungsbereich der EU hinaus wirkt.[7] Diese schützt klassisch die analogen Menschenrechte, darunter in Art. 8 die „Achtung der privaten Sphäre" und damit das Privat- und Familienleben, die Wohnung und den Briefverkehr. In seiner Rechtsprechung hat der Europäische Gerichtshof für Menschenrechte hieraus informationelle Schlussfolgerungen gezogen, die denen des BVerfG und des EuGH entsprechen.[8]

Das Kapitel des normativ gewährleisteten Grundrechtsschutzes öffneten Landesverfassungen deutscher Bundesländer (Nordrhein-Westfalen 1978, Saarland 1985) sowie anderer europäischer Staaten v.a. seit den 90er-Jahren.[9] Trotz einiger politischen Bestrebungen schaffte es das Grundrecht auf Datenschutz nicht ins GG. Dies erledigte sich dadurch, dass 2009 europaweit die europäische Grundrechte-Charta (GRCh) in Kraft trat, die in Art. 8 den „Schutz personenbezogener Daten" normativ festhält und zugleich die Zweckbindung, Betroffenenrechte und die unabhängige Kontrolle als wesentliche Rahmenbedingungen benennt. Die GRCh beschränkt sich hinsichtlich expliziter digitaler Grundrechte auf den Datenschutz, erweitert aber den Grundrechtekatalog um wesentliche, teilweise technisch bedingte dogmatische Neuerungen, etwa durch das Verbot des reproduktiven Klonens (Art. 3 Abs. 2 lit. d), die Verwendung des Begriffs „Kommunikation" beim Schutz des Post- und „Fernmeldegeheimnisses" (Art. 7), eine Präzisierung des Diskriminierungsverbots (Art. 21), durch Schutzvorkehrungen für besonders gefährdete Menschen (Ältere, Art. 25; Behinderte, Art. 26; Beschäftigte, Art. 27 ff.) und durch die Benennung von Schutzzielen (Gesundheitsschutz, Art. 35, Umweltschutz, Art. 37, Verbraucherschutz, Art. 38). Keine digitale, aber eine informationelle Neuerung ist das Recht auf Zugang zu Dokumenten (Art. 42 GRCh) – ein Grundrecht, dem sich bis heute das BVerfG ohne Not verweigert hat.[10]

Einen Ansatz für normativ fixierten digitalen Grundrechtsschutz suchte eine Gruppe von Politikern und Wissenschaftlern mit einem Entwurf für eine „Charta der Digitalen Grundrechte der Europäischen Union" im Jahr 2016, der das Ziel verfolgt die Debatte um Grundrechte im digitalen Zeitalter zu initiieren und die bestehenden Grundrechte zu stärken und zu konkretisieren.[11] Thematisiert werden darin automatisierte Systeme und Entscheidungen („künstliche Intelligenz", Robotik, Art. 5), ein Recht auf „digitalen Neuanfang" (Art. 7 Abs. 4), die Sicherheit informationstechnischer Systeme (Art. 8), das Recht auf Zugang zu Kommunikations- und Informationsdiensten (Art. 10), Netzneutralität (Art. 11), Pluralität und Interoperabilität (Art. 12) sowie ein Recht auf Immaterialgüter (Art. 17). Die Diskussion hierüber hat die formellen Kanäle der Verfassungsgesetzgebung noch nicht erreicht. Wohl aber scheint auf einfachgesetzlicher Ebene innerhalb der EU hinsichtlich der Regelungsinhalte des Charta-Entwurfs ein gewisser Konsens zu bestehen, der sich darin äußert, dass eine Vielzahl von fortschrittlichen Initiativen in Kraft gesetzt oder zumindest in Angriff genommen wurden. Dies gilt für die Regulierung von Internetdiensten und der Digitalmärkte, der elektronischen Kommunikation (ePrivacy), der

sog. künstlichen Intelligenz, eines Datenraums für Gesundheit und Mobilität, des Whistleblowings sowie des Zugangs zu und der Vermarktung von Daten. Mit einer Digitalen Agenda für Europa 2020 werden weitere Aspekte politisch und rechtlich angegangen. Demgegenüber beschränkt sich z.B. auf nationaler Ebene der Koalitionsvertrag der rot-grün-gelben Bundesregierung in Deutschland auf Umsetzungsfragen ohne einen umfassenderen Ansatz beim digitalen Grundrechtsschutz zu suchen.[12]

2. Vorbild DSGVO

Für die internationale Verbreitung digitalen Grundrechtsschutzes hat die europäische Datenschutz-Grundverordnung (DSGVO) zentrale Bedeutung. Zwar hat schon zuvor der Europäische Gerichtshof (EuGH) mit dem Safe-Harbor-Urteil[13] die rechtliche Grundlage dafür geschaffen, dass es beim Grundrechtsschutz im Rahmen des grenzüberschreitenden Informationsaustauschs auf Gegenseitigkeit ankommt. Dem EuGH kommt auch der Verdienst zu, dass er mit seinem Privacy-Shield-Urteil[14] und seinem Gutachten zum kanadischen Passenger-Name-Record[15] darauf besteht, dass diese Gegenseitigkeitsverpflichtung nicht aus politischen Opportunitätserwägungen relativiert oder gar zurückgenommen wird.

Den konkreten Rahmen für eine Gegenseitigkeitsanerkennung digitaler Grundrechte setzt aber die DSGVO. Diese verbietet grundsätzlich den Austausch personenbezogener Informationen mit dem Ausland, wenn dort nicht ein hinreichender Grundrechtsschutz gewährleistet wird. Dieser Grundsatz kennt zweifellos – auch humanitär begründete – Ausnahmen. Doch schafft die DSGVO vor allem ein Instrumentarium, um den Grundrechtsschutz zu exportieren. Dabei macht sie sich den Umstand zu Nutze, dass die wirtschaftlich bedingte internationale Kooperation kaum noch ohne den Austausch personenbezogener Daten auskommt. Das stärkste Instrument ist der Angemessenheitsbeschluss (Art. 45 DSGVO), der das Ausland veranlasst den europäischen Grundrechtsschutz zumindest ansatzweise ins eigene Rechtssystem zu importieren. Dass inzwischen so unterschiedliche Staaten wie Japan und Brasilien diesen Weg gegangen sind, auch wenn es normative sowie vor allem administrative Defizite geben mag, zeigt die Bereitschaft dieser Länder dem Datenschutz durch Normsetzung eine erhöhte Verbindlichkeit beizumessen.

Für die Feststellung der Angemessenheit kommt es nicht darauf an, dass die zum Einsatz kommenden Instrumente mit ihren rechtlichen Zuordnungen und deren Ableitungen identisch zu denen der DSGVO sind. Von zentraler Bedeutung ist, dass das, was in Deutschland informationelle Selbstbestimmung genannt wird, im Ergebnis normativ gewährleistet und tatsächlich in der lokalen Kultur etabliert ist, wobei die Kulturen sich nicht nur unterscheiden können, sondern auch angesichts unterschiedlicher ökonomischer, sozialer und politischer Bedingungen sowie historischer Traditionen unterscheiden müssen. Es wäre weder den Menschen noch dem internationalen wirtschaftlichen Austausch gedient, wenn westeuropäische Bürgerrechtler versuchen würden ihr Verständnis und ihre Praxis des Grundrechtsschutzes in andere Staaten zu exportieren oder gar zu oktroyieren.

Strukturell unterscheiden sich die Kulturen informationeller Selbstbestimmung hinsichtlich der Beziehung des einzelnen Menschen zu den gesellschaftlich schützenden und geschützten Kollektiven – von der Familie über die Religionsgemeinschaft bis hin zur staatlichen Gemeinschaft. Bei aller Unterschiedlichkeit dürfen aber Minimalstandards bzgl. der seit Jahrzehnten anerkannten (analogen) Grundrechte nicht negiert werden, vom Gleichheitsgrundsatz (auch zwischen Mann und Frau), dem Recht auf körperliche Unversehrtheit bis hin zu den politischen Freiheiten. Das in Westeuropa dominierende Primat der Wirtschaft darf aber in keinem Fall zur Grundlage für die Feststellung einer Grundrechtsangemessenheit gemacht werden. Es mag für westliche Kulturen prägend sein, hat aber jenseits der individuellen Selbstbestimmung keine grund- oder menschenrechtliche Rechtfertigung.

Soweit eine Feststellung der Angemessenheit nicht gelingt, wie etwa mit den USA, hält die DSGVO weitere Instrumente bereit, mit denen zumindest grundrechtliche Brückenköpfe im Ausland gesetzt werden können, insbesondere die Standarddatenschutzklauseln sowie die Binding Corporate Rules (Art. 46, 47 DSGVO).

Es gibt auch Staaten, bei denen eine Angemessenheit des Grundrechtsschutzes in keinem Fall festgestellt und auch über organisatorische Instrumente nicht hergestellt werden kann. So ist etwa die Datenverarbeitung in der Volksrepublik China momentan weder denkbar noch akzeptabel. Und seitdem sich China Hongkong rechtlich und politisch einverleibt hat, gilt dies auch für diesen Standort. So ist es nach der DSGVO z.B. schlicht unzulässig Genanalysen von Schwangeren im Interesse einer Trisomie-Feststellung in Hongkongs Laboren in Auftrag zu geben.[16]

3. Informationelle Selbstbestimmung und Repression

Das Grundrecht auf Datenschutz ist kein für sich alleinstehendes Recht. Schon in der dieses Grundrecht begründenden Volkszählungsentscheidung leitete das BVerfG das Recht auf informationelle Selbstbestimmung aus dem allgemeinen Persönlichkeitsrecht ab, also aus der Würdegarantie des Art. 1 Abs. 1 GG und der allgemeinen Handlungsfreiheit des Art. 2 Abs. 1 GG. Die „Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen" sollte einen dienenden Charakter haben, nämlich individuell die Freiheitsrechte des Einzelnen zu sichern und gesellschaftlich den Schutz des „auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens" sicherzustellen. Das BVerfG erwähnte dort ausdrücklich politische Grundrechte, konkret die auf „Teilnahme an einer Versammlung oder einer Bürgerinitiative" (Art. 8, 9 GG), beschränkte das Recht auf informationelle Selbstbestimmung aber nicht hierauf. Es betonte, dass die informationelle Erfassung zum Verzicht jedes Grundrechts führen könne.[17]

Dabei nannte das BVerfG keine weiteren Belege dafür, dass Datenüberwachung zu einem Grundrechtsverlust

führen kann, sondern setzte dies voraus: Deutsche Staaten hatten genügend Beispiele geliefert, wie Datenerfassung zum Grundrechtsverlust und zur Demokratiegefährdung führt. In der Bundesrepublik waren entsprechende Erfahrungen im Nationalsozialismus und im realen Sozialismus der DDR präsent. Es bedurfte keines Psychologisierens, um die zerstörerische Kraft staatlicher Kontrolle für Freiheitsrechte und Demokratie zu plausibilisieren.

Dies mag sich knapp 40 Jahre später anders darstellen, nachdem die Repression der DDR-Stasi nicht mehr im Bewusstsein und die Erinnerung an den Nationalsozialismus für viele verblasst ist. Die Bedeutung von Freiheitsrechten hat sich für viele Menschen immer mehr darauf reduziert hemmungslos konsumieren zu können und folgenlos Deutschland eine Merkel-Diktatur nennen zu dürfen. In diese Zeit drängt sich nun die Zeitenwende, mit der ein Totalitarismus à la Russland oder China präsent wird. Globale Konflikte, etwa die Klimakatastrophe, die Umweltzerstörung, das Artensterben, die Überbevölkerung oder der Welthunger machen den Menschen im Westen bewusst, dass Konsum und Narrenfreiheit keine Selbstverständlichkeit sind; der Ukrainekrieg schafft diese Botschaft täglich in die Nachrichten.

Diese Bewusstseinserweiterung bleibt partiell. Gerade die gesellschaftspolitischen, teils globalen und durchgängig komplexen Herausforderungen führen dazu, dass die Menschen ihre Wahrnehmung von Grundrechten auf einen individuellen Hausgebrauch reduzieren. Angesichts der allgegenwärtigen Probleme scheint die Wahrung des Datenschutzes von vielen als Luxus-Problem wahrgenommen zu werden. Der Konsumismus, der sich seit Jahrzehnten immer weiter verstärkt hat und an dem gerade private Digitalunternehmen einen beschleunigenden Anteil haben, tut das Seine, um Datenschutz von der Tagesordnung zu streichen. Die Folge ist, dass das Thema gerade in Deutschland – dem Land, das über Jahrzehnte beim Datenschutz als Vorreiter auch im gesellschaftlichen Bewusstsein wahrgenommen wurde – in der Rangordnung verliert. Es gibt nicht nur ein Datenschutz-Paradoxon der Verbraucher, die ihre digitale Privatsphäre als stark schützenswert ansehen und die zugleich relativ bedenkenlos datenschutzwidrige digitale Medien nutzen. Es gibt dieses Paradoxon auch bei Behörden, die den Datenschutz hochhalten, um Transparenz und Kontrolle bei sich zu verhindern und zugleich bedenkenlos datenschutzwidrig Social Media zum Einsatz bringen. Viele in den deutschen Behörden und in der Politik haben offenbar immer noch nicht erkannt, welche zerstörerische Kraft von datenschutzwidrigen und damit illegalen Geschäftsmodellen wie Facebook ausgeht.[18]

4. Digitalisierte Grundrechte

Die Beschränktheit des Bewusstseins über den Datenschutz ändert nichts an dessen freiheitssichernden Funktion in einer digitalisierten Informationsgesellschaft. Es ist offenbar, dass in Gesellschaften, in denen religiöse Verfolgung und Diskriminierung droht, zur Religionsfreiheit (Art. 4 GG, Art. 10 Abs. 1 GRCh) gehören muss die eigene Religionszugehörigkeit geheim halten zu können. Der Schutz vor politischer Verfolgung des Asylrechts (Art. 16a Abs. 1 GG, Art. 18 GRCh) muss einher gehen mit einem „Asylgeheimnis“, das insbesondere vor einer Datenpreisgabe gegenüber den politischen Verfolgern bewahrt.[19] Welche dramatischen Folgen informationelle Erfassung nach einem Systemwechsel von einer fragilen Demokratie hin zu einem religiösfundamentalistischem Gewaltsystem haben kann, zeigen jüngst Erfahrungen in Afghanistan.[20] Dass der Schutz der Wohnung (Art. 13 GG, Art. 7 GRCh) eine informationelle Komponente hat und deshalb der Lausch- und Späheingriff unzulässig ist, wurde vom BVerfG eindrucksvoll nach dem gesetzlichen Angriff auf das Heim als individuellen Rückzugsraum dargelegt.[21] Bei der Zurückweisung der Einschränkungen von Mobilität und Freizügigkeit (Art. 11 GG) durch das BVerfG über das Instrument der Kfz-Kennzeichenerfassung[22] oder durch den Europäischen Gerichtshof (EuGH) über das Instrument des Passenger-Name-Records[23] beriefen sich die obersten Gerichte auf das Datenschutzgrundrecht ohne dessen analoge Relevanz zu betonen. Entsprechendes gilt für Standortdaten und das Telekommunikationsgeheimnis in einer Vielzahl von Entscheidungen des EuGH und europäischer Verfassungsgerichte zur Vorratsdatenspeicherung.[24] Die Parallelität des Datenschutzes mit dem Schutz des Fernmelde- bzw. Telekommunikationsgeheimnisses (Art. 10 GG, Art. 7 GRCh) wurde in vielen höchstrichterlichen Entscheidungen betont.[25]

Das BVerfG hat sich innovativ dadurch hervorgetan, dass es – auch aus dem allgemeinen Persönlichkeitsrecht – ein neues digitales Grundrecht abgeleitet hat: das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, auch „Computer-Grundrecht“ genannt.[26] Damit zieht das BVerfG konsequent einen Schluss aus dem Umstand, dass in unserer digitalisierten Gesellschaft nicht mehr nur die Wohnung (räumlich) und die Familie (sozial) einen höchstpersönlichen Schutzbereich darstellen müssen, sondern auch die von einem Menschen privat genutzten informationstechnischen Digitalgeräte. Dass das Patientengeheimnis als spezifischer Datenschutz auch dem Schutz der beruflichen Verschwiegenheit (Art. 12 GG, Art. 15 GRCh) sowie des Lebens und der körperlichen Unversehrtheit (Art. 2 Abs. 1 GG, Art. 3 GRCh) dient, hat eine uralte Tradition.[27] Auch der Schutz der Familie (Art. 6 GG, Art. 7 GRCh) hat informationell einen abwehrenden Charakter.[28]

Neben den Freiheitsrechten bestehen zwischen den Gleichheitsrechten (Art. 3 GG, Art. 20, 21, 23 GRCh) bzw. dem Schutz vor Diskriminierung elementare Wechselwirkungen zum Grundrecht auf Datenschutz. Dies findet seinen normativen Ausdruck in dem besonderen Schutz sensitiver Daten in Art. 9 DSGVO, wonach die Verarbeitung von „Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung“ einer spezifischen und erhöhten Legitimation bedürfen.

Selbst Sicherungen der Rechtsstaatlichkeit und des gerichtlichen Rechtsschutzes (Art. 19 Abs. 4 GG, Art. 47 GRCh) bedürfen einer informationellen Flankierung. Prozessuale Absicherungen sind die Unschuldsvermutung, der Nemo-Tenetur-Grundsatz[29] sowie die Ansprüche auf Resozialisierung und auf ein faires Verfahren (Art. 48, 49 GRCh). Art. 10 DSGVO, der die Verarbeitung von Daten über Verurteilungen und Straftaten einschränkt, basiert auf entsprechenden Erwägungen.

Mit dem Internet und den dort zum Einsatz kommenden Social Media hat das Verhältnis der Meinungs- und Informationsfreiheit (Art. 5 GG, Art. 11 GRCh) zum Datenschutz bzw. das Verhältnis zwischen Verantwortlichkeit und Anonymität besondere Relevanz erhalten: Die unbeobachtete Informationsbeschaffung und freie Meinungsäußerung sind eine Grundvoraussetzung für den demokratischen und angstfreien Diskurs. Zugleich führt die Anonymität und globale Verbreitbarkeit von Hass- und Falschbotschaften, also von Hatespeach und Fakenews, zur wohl derzeit größten Gefahr weltweit für die Demokratie und für das Persönlichkeitsrecht von Betroffenen. Beredtes Zeugnis hierfür ist die Aufpeitschung zum Rassenhass durch Facebook etwa in Myanmar gegen die Rohinjas[30] oder die diskurszerstörende Wirkung dieser Plattform auf den Philippinen.[31]

Der EuGH[32], das BVerfG[33] und nationale Gerichte haben sich in vielen Entscheidungen zum Verhältnis von Meinungsfreiheit und Persönlichkeitsschutz geäußert. Es ist ein bisher nur in Ansätzen – etwa mit dem Netzwerkdurchsetzungsgesetz und geplant mit dem Digital Services Act[34] – gelöstes Regulierungsproblem der verantwortungsvollen Freiheitsicherung des für die Demokratie unabdingbaren Kampfes um Wahrheit und Meinungen. Gerade insofern unterscheiden sich autoritäre und totalitäre Staaten wie Russland und China, aber auch weniger entwickelte Staaten wie Iran, von Demokratien, dass dort sowohl die Informationsbeschaffung als auch die Informationsverbreitung kontrolliert und im Zweifelsfall zensiert und sanktioniert werden.

Schon bei den analogen Grundrechten gilt das, was für digitale Grundrechte hinsichtlich der Rolle des Staates noch wichtiger ist, da individueller Schutz für Betroffene hier ohne fremde Hilfe oft unmöglich ist: Die Grundrechte sind nicht nur Abwehrrechte vor hoheitlichen Eingriffen, sondern begründen auch Ansprüche auf Teilhabe und auf staatliche Gewährleistungen einschließlich des Schutzes vor Eingriffen durch Private. Dies gilt insbesondere für den Schutz vor Übergriffen durch globale Digitalkonzerne, aber auch durch einzelne Personen, die sich z.B. im Netz mit Fakenews und Hatespeach über andere Menschen hermachen. Es geht um eine staatliche Schutzpflicht, über die verhindert werden muss, dass Selbstbestimmung durch Informationsverarbeitung in Fremdbestimmung verkehrt wird.[35] Wie diese Schutzpflicht umgesetzt wird, bleibt aber weitgehend dem Gesetzgeber überlassen.

5. Der Datenschutz als Menschenrecht?

Die Enthüllungen Edward Snowdens zu den weltweiten Überwachungsaktivitäten insbesondere des US-Geheimdienstes NSA (National Security Agency) und des britischen GCHQ (Government Communications Headquarters) hatten eine weltweite Diskussion über Überwachung und Datenschutz zur Folge. So offensichtlich es war, dass die Aktivitäten von NSA und GCHQ nicht in Ordnung sind, so wenig klar war aus Völkerrechtssicht, weshalb. Es fehlt eine klare, weltweit geltende normative Grundlage. Auf Initiative von Brasilien und Deutschland beschloss der Menschenrechtsausschuss der Vollversammlung der Vereinten Nationen am 26.11.2013 die Resolution „Recht auf Privatheit im digitalen Zeitalter". Darin wird Bezug genommen auf das Recht auf Privatheit, wie es in Art. 12 der Allgemeinen Erklärung der Menschenrechte und in Art. 17 des Internationalen Paktes für zivile und politische Rechte gewährleistet ist. Sie erkennt an, dass der Schutz der Privatheit „wichtig für die Verwirklichung des Rechts auf freie Meinungsäußerung und auf unbeeinträchtigte Überzeugung sowie eine der Grundlagen einer demokratischen Gesellschaft ist" und bestätigt, „dass dieselben Rechte, die Menschen offline haben, einschließlich des Rechts auf Privatheit, auch online geschützt werden müssen".[36]

Die Erwartung bzw. Hoffnung, dass die Enthüllungen von Snowden und die dadurch ausgelösten Diskussionen global eine Initialzündung für die Schaffung eines internationalen digitalen Grundrechtsschutzes würden, ist inzwischen verflogen. Dies hat nicht nur seinen Grund darin, dass Mächte wie China oder Russland sich einer solchen Entwicklung entgegensetzen. Hinderlich für eine Verbreitung des Gedankens eines digitalen Grundrechtsschutzes waren und sind auch die USA, selbst unter einer von Barack Obama oder Joe Biden geführten Administration. Es hat sich nichts daran geändert, dass die US-Administration Verfechter des digitalen Grundrechtsschutzes wie Edward Snowden verfolgt statt diesen zu danken und diese zu ehren.

Die Diskussion in den USA war und ist geprägt von Abwehrkämpfen gegen europäische grundrechtliche Begehrlichkeiten. Dies ist erstaunlich, zumal die Ursprünge der Debatten um digitale bzw. informationelle Grundrechte in den USA zu finden sind.[37] Die verfassungsrechtliche Konkretisierung digitaler Grundrechte allgemein und von „Privacy" spezifisch scheiterte bisher an den sicherheitspolitischen Interessen der US-Administration sowie den ökonomischen Interessen der US-Internetwirtschaft. Einer der europäischen Verfassungsentwicklung vergleichbaren Weiterschreibung von Grundrechten steht in den USA ein für europäische Juristen schwer nachvollziehbares Verständnis von „Privacy" entgegen. Dieses nimmt auf der höchsten Ebene des Supreme Courts Digitalisierung nicht zur Kenntnis. Bis zur jüngsten Wende im Rahmen der Entscheidung des Supreme Court zur Abtreibung vom 24.06.2022[38] vertrat dieses Gericht mit der Entscheidung „Roe vs. Wade" 1973 z.B. die Ansicht, dass das analoge Recht auf Abtreibung unter „Privacy" zu subsumieren sei.[39] Die Interessenlage hat sich in den USA seit 2013 nur wenig geändert: Das überbordende Interesse an staatlich herzustellender informationeller Sicherheit ist ungebrochen. Wohl ist eine zunehmende Skepsis gegenüber den Machtansprüchen der US-Digital-Konzerne feststellbar. Dies zeigt sich auch in einer

Vielzahl von Gerichtsentscheidungen in den USA. Diese können aber – anders als in Europa – nicht auf eine konsistente Verfassungsrechtslage zurückgreifen.

In Staaten außerhalb der westlichen Hemisphäre kann von einer Anerkennung des Datenschutzes als Menschenrecht keine Rede sein. Datenschutzgesetze in China[40] oder in Russland dienen nicht oder nur begrenzt dem Schutz des Individuums, allenfalls in dessen Rolle als Verbraucher. Das Primat staatlicher Kontrolle gilt mehr denn je und wird in immer mehr digitalen Kontrollinstrumenten umgesetzt. Das weltweite Bekenntnis zu Menschenrechten nach dem zweiten Weltkrieg war immer brüchig, ist aber brüchiger geworden und erstreckt sich noch nicht mal im Ansatz auf den digitalen Raum.

6. Totalitarismus auf dem Vormarsch?

Es war eine allgemein anerkannte Vorstellung zu Beginn dieses Jahrtausends, dass mit der Verbreitung des globalen Internets ein weltweiter Informationsaustausch ermöglicht wird, was letztlich Demokratisierung zur Folge haben würde. Diese Hoffnung wurde durch den von digitalen Medien getriebenen, im Dezember 2010 beginnenden sog. arabischen Frühling befeuert. Von dieser Hoffnung ist wenig geblieben. Nach einer Reform- und Öffnungsphase ab 1978 hatte sich China unter Xi Jinping schon viel früher immer mehr zu einem allüberwachenden Überwachungsstaat entwickelt. Der Austausch über das WorldWideWeb wurde behindert, das nationale Netz einer strengen Zensur unterworfen, digitale Technik wurde zur Totalkontrolle der Bevölkerung eingesetzt. Seit dem Massaker auf dem Tian'anmen-Platz in Peking 1989 konnte dies für jeden, der dies wissen wollte, erkennbar sein. In Xinjiang betreibt die chinesische Regierung mit hohem technischen Aufwand die Zerstörung des Lebens und der Kultur der Uiguren.

Ihren Einsatz der Digitaltechnik exportiert China erfolgreich in die ganze Welt. Chinesische Unternehmen sind auf den digitalen Märkten aktiv, sei es mit Tiktok[41] im Bereich der Social Media, mit Alibaba im Bereich des Online-Handels, mit Huawei und später Xiaomi bei Smartphones und mit Huawei bei mobiler Netzwerktechnik. Die chinesischen Unternehmen unterwerfen sich umfassend den Kontrollwünschen der regierenden kommunistischen Partei, der Sicherheitsbehörden und des Militärs. Es war ein dem digitalen Grundrechtsschutz wenig zugeneigter US-Präsident Donald Trump, der sich dem chinesischen digitalen Expansionsstreben entgegenstellte.

Die arabischen Staaten haben sich fast durchgängig zu High-Tech-Überwachungsgesellschaften entwickelt. Der schiitisch-islamische Iran schottet sich ähnlich wie China ab. Das sunnitische Saudi-Arabien oder die Vereinigten Arabischen Emirate verfolgen totalitäre Kontrollstrategien gegenüber ihrer Bevölkerung. Russland, das sich um die 2000er-Jahre noch dem Westen geöffnet hatte, verschärft seitdem Überwachung und Zensur und bietet Cyberkriminellen nicht nur eine sichere Heimstatt, sondern Lohn und Brot. Mit dem kriegerischen Einfall in die Ukraine befreite sich das Russland Putins von jeglichen bürgerrechtlichen Fesseln und profiliert sich als Hauptproduzent von Hass und realitätsungetrübter Propaganda.

7. Herausforderungen auch in demokratischen Staaten

Auch in westlichen Ländern und Europa ist es mit dem digitalen Grundrechtsschutz nicht zum Besten gestellt: Trump schafft es seit Jahren unter Einsatz digitaler Medien die US-Gesellschaft zu spalten. In Großbritannien wurde – auch Dank einer auf Fakenews basierten Medienkampagne – die politische Loslösung von der EU durchgesetzt. In Polen und Ungarn werden Medien und Justiz immer mehr gleichgeschaltet. Selbst vor der Gleichschaltung der Datenschutzkontrolle machte der ungarische Ministerpräsident Orban nicht halt.[42]

Die aktuellen Entwicklungen haben in westlichen Gesellschaften zur Folge, dass das Primat der Wirtschaft nicht mehr alleinbestimmend ist und Werteorientierungen an Bedeutung gewinnen. Gesellschaftlicher Optimismus ist zweifellos als individuelle Grundhaltung begrüßenswert. Doch die Annahme, dass die Geschichte durch den weltweiten – ökonomischen wie informationellen – Austausch zwangsläufig zu mehr Frieden und Freiheit führt, hat sich als Irrglaube und gefährliches Wunschdenken erwiesen. Spätestens mit dem Einmarsch Russlands in die Ukraine ist offenbar, dass Frieden, Freiheit, Demokratie und eben auch informationelle Selbstbestimmung immer wieder neu erkämpft werden müssen. Bei diesem Kampf müssen angesichts der oft bestehenden globalen Abhängigkeiten und Verflechtungen diese immer im Blick bleiben.

Seit ca. fünf Jahren wird im Bereich der Digitalisierung nun auch in Westeuropa verstärkt auf Souveränität gesetzt.[43] Es ist vielleicht eine Ironie der Geschichte, dass das Anfang der 70er-Jahre in ökologischen alternativen Zirkeln verbreitete Motto des „small is beautiful" informationstechnisch ein Revival erlebt: Offline ist besser als online, dezentral besser als zentral, regional besser als international. Das Motto steht aber oft im praktischen Widerspruch zu digitalen Realitäten und Notwendigkeiten: Vernetzung zwingt zu globalen Standards und größtmöglicher Einheitlichkeit, Cybersicherheit muss sich weltweit am jeweils höchsten Stand orientieren. Und schließlich ist es immer (noch) eine nicht zu ignorierende Realität im globalen Digitalwettbewerb: „The winner takes it all".

Gefordert ist daher eine komplexe und differenzierte Digitalpolitik im Dienste des Grundrechtsschutzes. Trotz des weitverbreiteten Geredes über digitale Disruption kann und darf insofern keine disruptive „Zeitenwende" erfolgen, wohl aber sind Prioritäten neu zu setzen. Das Primat der Wirtschaft muss dem Primat der Politik weichen. Das Primat des Verarbeiters, ob Unternehmen oder Staat, muss dem Primat des gemeinschaftsverpflichteten Individuums weichen.

Digitale Souveränität ist oft national realistisch nicht mehr möglich; europäische Ansätze drängen sich auf. Europa ist nicht nur eine Werte-, sondern auch eine Rechtsgemeinschaft. Die EU-Kommission nimmt insofern mit ihrer Digitalstrategie und den darin enthaltenen Rechtsinstrumenten richtige Weichenstellungen vor. Der europäische Ansatz vermeidet einen nationalistischen Zungenschlag. Ein Streben nach europäischer Souveränität bewahrt und fördert zugleich die politische und rechtliche Integration Europas.

Beim digitalen Grundrechtsschutz gibt es nicht nur Schwarz und Weiß. Europa ist beileibe nicht nur auf der Seite des Guten, die USA, Russland und China sind nicht zwangsläufig auf der Seite des Bösen. Die europäischen Reaktionen auf die Snowden-Enthüllungen zeigten europäische, im Gleichklang mit den USA stehende Überwachungsinteressen auf, mit dem Wunsch nach Teilhabe an den US-Erkenntnissen und dem Ziel die digitale Technik zur Herrschaftserweiterung und -sicherung nach innen wie nach außen zu nutzen. Zu verlockend sind Vorratsdatenspeicherungen oder die Inhaltskontrolle der Internet-Kommunikation, um so legitime Ziele wie die Bekämpfung von Terrorismus oder Kinderpornografie zu verfolgen. Europa hebt sich allenfalls graduell von anderen Staaten in der Welt ab, insbesondere Dank einer agilen Zivilgesellschaft und relativ unbestechlicher Gerichte.

Die aktuelle ökonomische Antwort auf die Globalisierung lässt sich auf das Digitale übertragen: Es kann und es darf keine vollständige Abschottung geben. Dies gilt wegen des sich entwickelnden technischen und ökonomischen Know-hows, das sich zuletzt v.a. in den USA und China weiterentwickelt hat und wovon Europa lernen kann. Mitte des 20. Jahrhunderts setzte Deutschland noch technologische Standards. Auch sind die Zeiten wie Ende des 20. Jahrhunderts vorbei, als China von westlichen Staaten v.a. kopierte. In Sachen Big Data, sog. künstlicher Intelligenz sowie Vernetzung kann Europa lernen und muss lernbereit werden bzw. bleiben. Europa kann für das globale Digitalwissen sein Grundrechts-Know-how einbringen, etwa zu Privacy-Enhancing-Technologies und zu kooperativen Verarbeitungsmethoden.

8. Grundrechtsschutz und Digitalwirtschaft

Hinsichtlich der Hardware-Produktion wird die Digitalwirtschaft immer von Rohstofflieferungen abhängig sein. Dies hindert Produzenten bzw. Gesellschaften nicht die Einhaltung von Grundrechtsstandards entlang der Lieferketten normativ einzufordern und zu kontrollieren – bei allen praktisch notwendigen Kompromissen. Eine zentrale Lehre aus dem Ukraine-Konflikt ist, dass die eigene Bestimmungsmacht über wesentliche Produktionsbereiche gewahrt bzw. wieder hergestellt werden muss. Es ist einfach klug Standortentscheidungen zu Halbleiterfabriken oder die Herstellung von Produkten für den digitalen Alltag wie insbesondere für die kritische Infrastruktur nicht nur von den aktuellen Produktionskosten bestimmen zu lassen. Erwägungen der Souveränität und der Grundrechtskonformität über die gesamte Lieferkette sind einzupreisen. In Europa vorhandene Ressourcen können gehoben werden. Bei der Fertigung von Halbleitern liegt der Marktanteil Europas derzeit bei ca. 10%.[44] Bestehende Ressourcen des Recyclings wurden bisher vernachlässigt; sie sind nicht nur eine Frage des Umweltschutzes, sondern auch eine Frage der Souveränität und damit letztlich des digitalen Grundrechtsschutzes.

Was für die Hardware gilt, gilt verstärkt für die Softwareproduktion und -pflege. Im Interesse einheitlicher Standards ist die Produktion von Software-Bestandteilen an fernen Standorten oft naheliegend. Das Prinzip der datenschutzrechtlichen Verantwortlichkeit setzt aber voraus, dass das Know-how über die wesentlichen Funktionalitäten vor Ort vorhanden ist. Wird dieses Know-how von einem Software-Lieferanten verweigert, so ist der Nichteinsatz dieser Software die einzige vernünftige Antwort. Wie weit die Praxis hiervon entfernt ist, zeigen die Weigerung Facebooks angesichts der gemeinsamen Verantwortlichkeit z.B. von Fanpages ein transparentes und dadurch datenschutzkonformes „Addendum" zur Verfügung zu stellen, die Weigerung des Auftragsverarbeiters AmazonWebServices (AWS) den Auftraggebern in die Tiefen seines Cloud-Betriebs Einblick zu gewähren oder die Weigerung von Google die Algorithmen ihrer Suchmaschine offenzulegen.

Die EU versucht mit ihrer Digitalstrategie über Regulierungen normativ die Hoheit über die Datenverarbeitung wiederherzustellen und parallel dazu europäische Alternativen insbesondere zu US-amerikanischen Angeboten zu entwickeln und zu etablieren. Die aktuellen Abhängigkeiten sind gewaltig: 90% der europäischen Daten werden in Clouddiensten von US-Konzernen geführt.[45] Europäische Kooperationen mit US-Anbietern müssen nicht ausgeschlossen sein, doch sollte dabei eine gleiche Augenhöhe bestehen.

Wirtschaftsrechtliche Grundsätze lassen sich auf den digitalen Grundrechtsschutzes übertragen: So sind Monopole Gift für Grundrechte; Pluralität und ein vielfältiges Angebot sind förderlich. Dies gilt erst recht, wenn der Nachweis von Grundrechtskonformität zu einer Voraussetzung für den Marktzugang gemacht wird. Mit dem Digital Markets Act und dem Digital Services Act versucht die EU diese Erkenntnis in die Realität umzusetzen.

Die Rolle der USA ist eine besondere. Mit der Regierung Trumps wurde Europa signalisiert, dass Wertegemeinsamkeiten mit der US-Politik nicht selbstverständlich sind. Insofern muss es ein Ziel Europas sein Souveränität auch gegenüber den USA zu erlangen. Dieses Bewusstsein ist insofern in Europa noch entwicklungsfähig und -bedürftig. Zugleich sollte Europa seine Bemühungen verstärken hinsichtlich der Umsetzung digitaler Grundrechte Gemeinsamkeiten mit den USA herzustellen. Angesichts des sich verstärkenden Systemgegensatzes insbesondere zu China sollten die USA ein gesteigertes Interesse an einer eigenen starken Grundrechtsposition entwickeln und insofern mit Europa einen Schulterschluss suchen. Dass dem eine äußerst immobile Verfassungslage in den USA entgegensteht, ist ein Hindernis, schließt diese Annäherung aber nicht aus.

Die EU ist – anders als die USA – in Bezug auf Sanktionen gegenüber Unternehmen, die an grundrechtswidrigen Überwachungsaktivitäten beteiligt sind oder sein können, zurückhaltend. Die Trump-Administration setzte das Unternehmen Huawei 2019 auf eine schwarze Liste, was selbst US-Unternehmen daran hindert mit dem chinesischen Konzern Geschäfte zu machen. Dies gilt auch für Google als bis dahin wichtigster Software-Zulieferer für Huawei-Smartphones.[46] Die britische Regierung unter Boris Johnson schloss sich an.[47] Für beide Politiker waren nicht grundrechtliche, sondern strategische Erwägungen ausschlaggebend. Die EU versucht – zurückhaltender – nur zu vermeiden, dass über eine Integration von Huawei-Produkten beim Aufbau des

5G-Mobilfunknetzes chinesische Überwachungsschnittstellen entstehen.

Jüngstes Beispiel für eine Sanktionierung grundrechtszerstörender Überwachungssoftware ist das israelische Unternehmen NSO mit seinem Pegasus-Programm, das auch von den USA auf eine Sanktionsliste gesetzt wurde.[48] In Deutschland veranlassten Experten des Chaos Computer Clubs (CCC) und der Gesellschaft für Freiheitsrechte (GFF) ein Verfahren gegen Finfisher als Anbieter von Überwachungssoftware wegen eines Verstoßes gegen das Außenwirtschaftsgesetz.[49] Die am weitesten gehende Initiative trifft den chinesischen Hersteller und Weltmarktführer bei Videoüberwachungssystemen Hikvision, den die USA u.a. wegen seiner Beteiligung bei der Unterdrückung der Uiguren in Xingjiang auf eine Liste der „Special Designated Nationals and Blockes Personen" (SDN) setzen möchte, was eine direkte wie indirekte ökonomische Totalblockade zur Folge hätte.[50]

9. Völkerrechtliche Bestrebungen

Die Resolution zum Datenschutzrecht im digitalen Zeitalter in Reaktion auf die Veröffentlichungen von Edward Snowden über die weltweite Bespitzelung durch die NSA und den GCHQ vom 20.11.2013 blieb in der UNO bisher ein Unikat.[51] Zwar ist eine verbindliche Fixierung von digitalen Grundrechten derzeit politisch eine Utopie. Dies sollte aber kein Grund sein Bemühungen in diese Richtung zu unterlassen. Entsprechende Initiativen zwingen die Regierungen sich mit den Fragen auseinanderzusetzen, sich hierzu zu verhalten und ablehnende Positionen zu begründen. Datenschutz und digitale Grundrechte sind ein Thema für die UNO, deren Aufgabe darin besteht – soweit erforderlich – normative Grundlagen für ein friedliches Zusammenleben auf unserer Welt zu gewährleisten. Dass eine Notwendigkeit für eine Fixierung digitaler Menschenrechte besteht, ist angesichts der oben dargestellten Entwicklungen und Konflikte offenkundig. Eine global übergreifende Realisierung eines Grundrechtestandards ist u.a. wegen des mittelfristig weiterhin zu erwartenden Widerstands von China und Russland unrealistisch. Regionale völkerrechtliche Initiativen, etwa in Lateinamerika, Afrika oder im pazifischen Raum, haben dagegen höhere Realisierungschancen. Dies gilt insbesondere, wenn diese, wie ursprünglich in Europa beim Datenschutz, mit wirtschaftlichen informationellen Interessen in Verbindung gebracht werden.

Während das Zugestehen von individuellen Rechten bisher wenige Fürsprecher findet, besteht hinsichtlich der Bekämpfung von Cyberkriminalität und des Cyber-Terrorismus eine weitgehend gleichgelagerte Interessenlage staatlicher Regierungen. Aktivitäten hierzu dienen nicht nur den Individuen, sondern auch der Wirtschaft und der Verwaltung. Kriminelle Cyberaktivitäten von Privatpersonen finden aber teilweise staatliche Unterstützung oder gehen direkt von staatlichen Einrichtungen, in der Vergangenheit etwa von Israel, Russland und China, aus. Dies ändert nichts an der zumindest teilweise bestehenden Interessenlage und dem Bedarf an einer überstaatlichen Kooperation und Normierung, was auch dem digitalen Grundrechtsschutz zugutekommt.

Die Verknüpfung von wirtschaftlichen Kooperationsvereinbarungen mit Anforderungen an Grundrechtsschutz, Rechtsstaatlichkeit und Demokratie kann künftig ein wichtiges Instrument dafür sein Globalisierung menschenrechtskonform zu gestalten. Dies gilt auch für Freihandelsabkommen, denen immer eine informationelle Komponente zukommt.[52] Entsprechende Anforderungen haben nicht nur eine Wirkung auf die ökonomischen Kooperationspartner, sondern zugleich auch eine Schutzwirkung für die heimische, rechtlich gebundene grundrechtskonform agierende Wirtschaft.

Vergleichbare Vorgehensweisen bieten sich im internationalen Sicherheits- und Finanzbereich an. Die sicherheitspolitische Kooperation etwa im Verkehrsbereich durch den Austausch von Passenger-Name-Records setzt die Wahrung grundrechtlicher Standards durch alle eingebundenen Vertragspartner voraus.[53] Entsprechendes gilt für Kooperationen bei der Kriminalitätsbekämpfung oder der Wahrung der öffentlichen Sicherheit.[54] Eine interessante neue Variante völkerrechtlicher Sanktionierung von Grundrechtsverletzungen brachte der Ausschluss russischer Banken vom Finanzdatenaustausch gemäß dem SWIFT-Abkommen nach dem russischen Einfall in die Ukraine.

Flankierend zu völkerrechtlichen Bestrebungen kann der digitale Grundrechtsschutz durch nationale oder supranationale Maßnahmen vorangebracht werden. So ist es ein irritierender Umstand, dass der Whistleblower Edward Snowden, der sich weltweit um mehr Transparenz bei digitalen Grundrechtsverstößen verdient gemacht hat, Asyl in Russland suchen musste und nur dort finden konnte. Regelungen zum Whistleblowing im Interesse des Grundrechtsschutzes und zum Schutz der Whistleblower schaffen nicht nur einen Rahmen für mehr Compliance im eigenen Land, sondern können auch rechtliche Grundlagen dafür schaffen, dass Verstöße gegen digitale Grundrechte in anderen Staaten transparent werden, und dass Auslieferungsersuchen zu Whistleblowern durch Verfolgerstaaten rechtlich abgewehrt werden können.[55]

10. Schlussbemerkung

Digitaler Grundrechtsschutz ging vom Recht auf informationelle Selbstbestimmung und vom Datenschutz aus, beschränkt sich aber schon längst nicht mehr hierauf. Nationale Regelungen waren der Anfang, inzwischen liegt der Schwerpunkt auf Regelungen der EU. Völkerrechtliche Instrumente sind noch rar. Angesichts der „Zeitenwende" ist die Deckung dieses Bedarfs weniger absehbar als noch vor wenigen Monaten. Das globale Internet mit den damit verbundenen Chancen auf Informationsaustausch und Kooperation droht mit autoritären, die Grundrechte leugnenden Motiven national zerstückelt zu werden.

Die globalen Herausforderungen etwa im Bereich Klima, Nahrungsversorgung oder Friedenswahrung sind aber auf den informationellen Austausch und auf Kooperation angewiesen. Dies macht globale Spielregeln dringender denn je. Auch wenn die Diskussionskonjunktur insofern wenig hergibt, ist eine Debatte über digitale Grundrechte auf globaler Ebene dringend nötig. Das sind wir nicht nur den Uiguren und den Menschen in Hongkong oder den Oppositionellen in Russland oder Belarus schuldig, son-

dern auch uns selbst in den westlichen Staaten, in Europa, in Deutschland. Die Debatte über das „Internet als rechtsfreier Raum" ist in Europa überwunden. Es gibt einiges zu tun, um zu verhindern, dass dieses Phänomen uns über globale Entwicklungen wieder einholt.

1 Hage/Traufetter, Bundesregierung verwehrt VW Garantien für Investitionen in China, www.spiegel.de 27.05.2022.

2 Deutscher Bundestag, Wissenschaftliche Dienste, Zu den Grundrechten in der Weimarer Reichsverfassung, 2008, https://www.bundestag.de/resource/blob/423610/86e3e9e8a4b42e4b72fbd25413f285cb/wd-3-215-08-pdf-data.pdf.

3 BVerfG, U.v. 15.12.183 – 1 BvR 209/83 u.a., NJW 1984, 419.

4 Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten, European Treaty Series No. 108, BGBl. II 1985, 538

5 Organisation für wirtschaftliche Zusammenarbeit und Entwicklung, BAnz. Amtl. Teil v. 14.11.1981, Nr. 215.

6 Ausführlich dazu Simitis in Simitis, Bundesdatenschutzgesetz, 8. Aufl. 2014, Einleitung, Rn. 151 ff., 194; Burkert in Roßnagel, Handbuch Datenschutzrecht, 2003, 85 ff.

7 Konvention zum Schutz der Menschenrechte und Grundfreiheiten, BGBl. 1954 II S. 14.

8 Siemen, Datenschutz als europäisches Grundrecht, 2006.

9 Weichert, CR 1992, 738; Simitis in Simitis, BDSG, 8. Aufl. 2014, § 1 Rn. 29.

10 Wegener, Der geheime Staat, 2006.

11 Überarbeitet 2018, https://digitalcharta.eu/.

12 Weichert, DANA 1/2022, 4 ff., 18 ff.

13 EuGH U.v. 06.10.2015 – C-362/14 (Schrems I), NJW 2015, 3151.

14 EuGH U.v. 16.07.2020 – C-311/18 (Schrems II), NJW 2020, 2613.

15 EuGH U.v. 21.06.2022 – C-817/19, EuGH G.v. 26.07.2017 – Gutachten 1/15, ZD 2018, 23.

16 Netzwerk Datenschutzexpertise, 30.07.2021, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2021_eluthia_previatest3.pdf.

17 BVerfG, U.v. 15.12.183 – 1 BvR 209/83 u.a., NJW 1984, 419, 422.

18 Hurtz/Kampf/Krause/Kreye/Mascolo/Obermaier, Whistleblowerin Francis Haugen, SZ 28.10.2021, 11; Wilkens, Facebook-Fanpage: Datenschutzbeauftragter eröffnet Verfahren gegen Bundesbehörde, www.heise.de 06.06.2022, Kurzlink: https://heise.de/-7132768.

19 Weichert in GK-AufenthG, Vorbem. AZRG Rn. 31.

20 Ehemalige GIZ-Mitarbeiter durch zurückgelassene Dokumente in Lebensgefahr, DANA 2/2022, 124.

21 BVerfG U. v. 03.03.2004 1 BvR 2378/98 u. 1 BvR 1084/99, NJW 2004, 999 ff.

22 BVerfG U. v. 11.03.2008 – 1 BvR 2074/05 u. 1 BvR 1254/07, NJW 2008, 1505; BVerfG U.v. 18.12.2018 – 1 BvR 142/15 u. 1 BvR 2795/09, 1 BvR 3187/10, NJW 2019, 827, 842.

23 EuGH U.v. 21.06.2022 – C-817/19, EuGH G.v. 26.07.2017 – Gutachten 1/15, ZD2018, 23.

24 Jüngst EuGH U.v. 05.04.2022 – C-140/20; TC Portugal U. v. 19.02.2022, DANA 2/2022, 126 f; BVerfG U.v. 02.03.2010 -- 1 BvR 256, 263, 586/08.

25 Jüngst EuGH U.v. 02.03.2021 – C-746/18; BVerfG U.v. 26.04.2022 – 1 BvR 1619/17.

26 BVerfG, U.v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822; zuletzt BVerfG, 26.04.2022 - 1 BvR 1619/17, NJW 2022, 1583.

27 Weichert in Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, Art. 4 Nr. 15 Rn. 4.

28 Vgl. auch Hoffmann/Luch/Schulz/Borchers, Die digitale Dimension der Grundrechte, 2015; Weichert, KJ 2014, 126.

29 Niemand darf gezwungen werden, sich selbst zu belasten, BVerfG B.v. 27.04.2010 – 2 BvL 13/07 Rn. 2.

30 Kreye, Rohingya verklagen Facebook, SZ 08.12.2021, 8.

31 „Ein Rennen gegen die Zeit", Interview von Obermaier/Obermayer mit Maria Ressa, SZ 20.02.2021, 40; generell Kreye, Der Blaue Planet, SZ 12./13.06.2021, 11 ff.

32 Z.B. EuGH U.v. 03.10.2019 – C-18/18; EuGH U.v. 24.09.2019 – C-507/17, NJW 2019. 3499.

33 BVerfG U.v. 06.11.2019 – 1 BvR 16/13; BVerfG U.v. 06.11.2019 – 1 BvR 276/17.

34 Roth, DANA 2/2022, 86 ff.

35 BVerfG, B.v. 17.07.2013 – 1 BvR 3167/08, Rn. 20, JZ 2013, 1157; BVerfG, B.v. 23.10.2006 – 1 BvR 2027/02, Rn. 29 ff.; JZ 2007, 576.

36 Abgedruckt bei Weichert, DuD 2014, 404.

37 Weichert, KJ 2014, 127 f; Weichert, RDV 2012, 113 ff.; zur sicherheitsbehördlichen Diskussion Arzt, Polizeiliche Überwachungsmaßnahmen in den USA, 2004; Grunwald, Datenerhebung durch das Federal Bureau of Investigation, 2008.

38 Supreme Court U.v. 24.06.2022, Dobbs v. Jackson Women´s Health Organization, No. 19-1392.

39 Supreme Court, U.v. 22.01.1973, Roe vs. Wade, 410 U.S. 113, Rn. 76 ff.

40 Chen/Han/Kipker DuD 20252 ff.

41 Krempl, TikTok bestätigt: Mitarbeiter in China können auf US-Nutzerdaten zugreifen, www.heise.de 03.07.2022, Kurzlink: https://heise.de/-7160888.

42 Rathke, Der EuGH und die Unabhängigkeit des ungarischen Datenschutzbeauftragten, 2014, https://www.juwiss.de/51-2014/.

43 Bizer in Lühr/Jabkowski/Smentek, Handbuch Digitale Verwaltung, 2019, S. 23 ff.

44 Book/Fahrion/Hage/Hesse/Knobbe/Sauga/Schulz/Traufetter, Die Ära der Deglobalisierung, Der Spiegel Nr. 26 v. 25.06.2022, S. 67.

45 Book/Fahrion/Hage/Hesse/Knobbe/Sauga/Schulz/Traufetter, Die Ära der Deglobalisierung, Der Spiegel Nr. 26 v. 25.06.2022, S. 67.

46 Hauck, Huawei versucht ein Smartphone-Comeback, SZ 26.10.2021, 16.

47 Giesen/Mühlauer, Huawei soll aus Großbritannien verschwinden, SZ 06.07.2020, 17.

48 Pegasus erschüttert israelische Politik, DANA 2/2022, 118f.

49 CCC-Experten enttarnen FinFisher-Überwachungssoftware, DANA 2/2020, 114 f.

50 Yang, Videoüberwachung: Die größte Überwachungsfirma, von der Sie nie gehört haben, www.heise.de 12.07.2022; Kurzlink: https://heise.de/-7158966.

51 United Nations General Assembly 20.11.2013, The Right to Privacy in the digital age, A/C.3/68/L45/45/ Rev.1; DANA 1/2014, 30 f.

52 Weichert DuD 2014, 850 ff.

53 EuGH G.v. 26.07.2017 – Gutachten 1/15, ZD2018, 23.

54 Hierzu kann die EU-Datenschutzrichtlinie für Justiz und Polizei 2016/680 als Vorbild angesehen werden.

55 Weichert KJ 2014, 131.

Achim Klabunde

Digitale Grundrechte im EU-Recht

Der Europarat als Garant der Menschenrechte

Während die EU und ihre Vorläuferorganisationen auf der Basis wirtschaftlicher Zusammenarbeit entstanden, waren Grundrechte und deren Sicherung und Durchsetzung in Europa von Anfang an zentral für die andere überstaatliche europäische Organisation, den Europarat (Conseil d'Europe, Council of Europe). Der Europarat, dem außer den EU-Mitgliedsstaaten noch viele weitere europäische Länder angehören, wurde bereits 1949 gegründet. Im Rahmen des Europarats wurde die europäische Menschenrechtskonvention (EMRK) verhandelt und 1950 beschlossen, die inzwischen von allen Mitgliedsstaaten des Europarates ratifiziert wurde.

Die EMRK legt die Menschenrechte fest, an die sich die Unterzeichnerstaaten binden, und etabliert den Europäischen Gerichtshof für Menschenrechte (EGMR), der darüber urteilt, ob Mitgliedsstaaten ihre Verpflichtungen nach der EMRK einhalten. Grundsätzlich können sich alle Betroffenen an den EGMR wenden, wenn sie glauben, dass ihre Rechte durch einen Mitgliedsstaat verletzt wurden. Sitz des EGMR und der anderen Organe des Europarats ist Straßburg.

Entstehung der EU als Wirtschaftsgemeinschaft

Die heutige Europäische Union entstand aus den Europäischen Gemeinschaften, die zunächst wirtschaftspolitische Ziele verfolgten, insbesondere die Europäische Gemeinschaft für Kohle und Stahl (EGKS, Montanunion) und die durch die Römischen Verträge von 1957 gegründete Europäische Wirtschaftsgemeinschaft (EWG). Da der Fokus der Zusammenarbeit zunächst auf wirtschaftliche Aktivitäten gerichtet war und letztlich das Ziel eines einheitlichen Binnenmarktes über alle Mitgliedsstaaten verfolgte, standen Fragen der Grundrechte ursprünglich nicht im Fokus des Rechtsrahmens.

Durch den Vertrag von Maastricht wurden 1993 die verschiedenen wirtschaftlichen Verträge zusammengefasst zum Vertrag über die Europäischen Gemeinschaften und so die Grundlagen für die Europäische Wirtschafts- und Währungsunion mit dem Euro als gemeinsamer Währung gelegt. Zugleich wurde der Vertrag über die Europäische Union geschlossen, die zunächst auf bestimmte Aufgabenbereiche außerhalb der wirtschaftlichen Regelungen konzentriert war, insbesondere die Zusammenarbeit in den Bereichen Inneres und Justiz und die Gemeinsame Außen- und Sicherheitspolitik (GASP).

Als bisher letzter Schritt der Entwicklung führte der Vertrag von Lissabon 2009 die Europäischen Gemeinschaften und die Europäische Union des Vertrags von Maastricht als einheitliche Organisation zusammen, unter dem Namen Europäische Union.

Verankerung der Grundrechte im EU-Recht

Mit dem Vertrag von Lissabon wurde die EMRK zum Bestandteil des EU-Rechts und zusätzlich ein eigener Grundrechtskatalog mit der Charta der Grundrechte der Europäischen Union (EU-Grundrechtecharta, EU-GRCh) als bindendes Recht hinzugefügt[1]. Damit sind jetzt alle Mitgliedsstaaten ebenso wie die Organe und anderen Behörden der EU bei der Anwendung des EU-Rechtes auf die Einhaltung der Grundrechte verpflichtet. Nachdem der in Straßburg ansässige EGMR bereits seit Jahrzehnten über die Einhaltung der Menschenrechte urteilt, kann jetzt auch der in Luxemburg ansässige Gerichtshof der Europäischen Union (Europäischer Gerichtshof, EuGH) bei seinen Urteilen über die Interpretation und Anwendung des EU-Rechtes die Einhaltung von Grundrechten bewerten. Dabei ist der EuGH auch in der Lage Rechtsakte der EU, also sowohl Richtlinien und Verordnungen als auch Entscheidungen der Kommission oder internationale Vereinbarungen der EU, zu überprüfen und bei Widerspruch zu den Grundrechten außer Kraft zu setzen. Der EuGH hat von dieser Möglichkeit auch Gebrauch gemacht und z.B. die Vorratsdatenspeicherungsrichtlinie, die Safe-Harbor- und Privacy-Shield-Entscheidungen der Kommission ebenso wie internationale Vereinbarungen zu Fluggastdaten aufgehoben.

Grundrechte im Internet

Datenschutz als genuin „Digitales Grundrecht"

Nach dem zweiten Weltkrieg hatten sich die Menschenrechte entwickelt, ohne dass technologische Aspekte dabei eine besondere Rolle spielten. Lediglich der Bedeutung von Kommunikationstechniken wie Telefonie wurde bereits mit der Einführung des Fernmeldegeheimnisses als Ergänzung zum Postgeheimnis Rechnung getragen. Demgegenüber entstand Datenschutz als Recht und später als Grundrecht erst als Reaktion auf die Einführung von Computern in der öffentlichen Verwaltung und der Wirtschaft. Auch wenn die Fähigkeiten der Computer in den 1970er-Jahren noch weit hinter dem heutigen Stand zurück blieben, erkannten die Befürworter des Datenschutzes bereits vor der allgegenwärtigen Datenerfassung und der weltweiten Vernetzung die potentiellen Auswirkungen der Kontrolle über personenbezogene Daten auf gesellschaftliche und wirtschaftliche Machtstrukturen.

Datenschutz war zunächst nicht als eigenständiges Grundrecht gedacht, sondern als Ableitung aus existierenden Grundrechten und als Notwendigkeit zu deren Sicherung. Datenschutzregeln entstanden zunächst in den nationalen Rechtssystemen. Dabei verboten viele Länder den Transfer von personenbe-

zogenen Daten aus ihrem Rechtsgebiet hinaus, um zu verhindern, dass ihre Bestimmungen durch Verarbeitung im Ausland umgangen wurden. Da diese Beschränkung als Hindernis für den wirtschaftlichen Austausch empfunden wurde, wurde versucht rechtliche Rahmen für grenzüberschreitenden Datenverkehr zu ermöglichen. Ein erstes rechtsverbindliches Instrument zu diesem Zweck war die Konvention 108 des Europarats, die 1981 Grundprinzipien des Datenschutzes festlegte. Zur Durchsetzung ihrer Rechte aus dieser Konvention steht den Betroffenen auch der Rechtsweg zum EGMR offen, der auch bereits eine Reihe von Urteilen zum Datenschutz getroffen hat. Die Konvention wurde 2018 überarbeitet, um sie an die technischen und wirtschaftlichen Entwicklungen anzupassen und auch die inzwischen in Kraft getretene Datenschutz-Grundverordnung (DSGVO) der EU zu berücksichtigen. Die Konvention 108 ist offen für Beitritt und Ratifizierung durch Staaten, die nicht Mitglied des Europarats sind, und wurde bereits von einigen afrikanischen und südamerikanischen Staaten unterzeichnet und ratifiziert.

Im Recht der Europäischen Gemeinschaften waren Regelungen zum Datenschutz zunächst Bestandteil der Regeln zum einheitlichen Wirtschaftsraum. Das erste Datenschutzinstrument, die Richtlinie 95/46, nennt in ihrem Titel zuerst den freien Fluss personenbezogener Daten innerhalb der Gemeinschaft und dann den Schutz natürlicher Personen bezüglich der Verarbeitung ihrer personenbezogenen Daten. Formelle Rechtsgrundlage der Richtlinie war der Artikel des EG-Vertrages über die Harmonisierung im Binnenmarkt. Erst mit dem Lissabon-Vertrag werden die Grundrechte ausdrücklich Bestandteil des EU-Rechts, durch den Bezug zur EMRK und die EU-GRCh. Die Charta nennt in ihrem Artikel 8 auch Datenschutz als eigenständiges Grundrecht, zusätzlich zum Recht auf Privatheit in Artikel 7.

Rechtsdurchsetzung im Netz

In der öffentlichen Diskussion wurde insbesondere seit der Einführung von Sozialen Medien häufig vom Internet als „rechtsfreiem Raum“ gesprochen. Diese Vorstellung wurde wohl einerseits von den eher romantischen Vorstellungen vom Internet als repressionsfreier Raum der Selbstorganisation beeinflusst, wie sie etwa von US-amerikanischen Aktivisten entwickelt wurden. Andererseits wurde der Eindruck der Rechtsfreiheit durch die tatsächliche Schwierigkeit der Durchsetzung von bestehenden Gesetzen bei Interaktionen im Internet hervorgerufen. Eigentlich sind und waren die bestehenden rechtlichen Vorschriften unabhängig davon anzuwenden, ob eine bestimmte Transaktion ganz oder teilweise durch das Internet vermittelt wurde. Solange alle daran beteiligten sich im selben Rechtsgebiet befinden, und dies auch festgestellt werden kann, können die unterschiedlichen Ansprüche auch mit den traditionellen Mitteln der Justiz durchgesetzt werden. Wenn aber die beteiligten Parteien in unterschiedlichen Jurisdiktionen arbeiten, stößt die Durchsetzung des Rechts auf erhebliche Hindernisse. Nicht immer ist es möglich den Standort aller Parteien überhaupt sicher festzustellen. Selbst wenn alle Beteiligten von demokratischen Rechtsstaaten aus agieren und die zuständige Exekutive und Judikative bekannt sind, und sogar wenn deren Justizsysteme auch prinzipiell gegenseitige Zusammenarbeit anstreben, können die praktischen Schwierigkeiten in vielen Fällen effektive Maßnahmen verhindern.

Selbst innerhalb der EU, die ja eine gemeinsame rechtliche Grundlage für einen alle Mitgliedsstaaten umfassenden Binnenmarkt hat, ist es nicht immer möglich rechtlich gegen Verstöße vorzugehen. Dies gilt sogar im Bereich der Grundrechte, insbesondere bei der freien Meinungsäußerung. Während in Deutschland die Verwendung von Nazi-Symbolen verboten ist, sind deutsche Versuche ein solches Verbot auf EU-Ebene einzuführen bisher gescheitert. In vielen weiteren Ländern gibt es keine Einschränkungen für solche Äußerungen im Netz. Die verschiedenen Aspekte der Grundrechte im Internet werden an anderer Stelle ausführlicher behandelt (Weichert, 2022[2]).

Unterschiedliche Auffassungen zum Datenschutz verdeutlichen die Schwierigkeiten bei der Durchsetzung von Grundrechten im Internet in ganz besonderer Weise. Auch wenn die USA bereits in den 1970er-Jahren Datenschutzprinzipien diskutierten und mit dem Federal Privacy Act von 1974 (FPA74) als einer der ersten Staaten überhaupt ein landesweit gültiges Datenschutzgesetz verabschiedeten, gibt es dort bis heute keinen umfassenden Schutz gegen die aus der Verarbeitung personenbezogener Daten erwachsenden Risiken für die Grundrechte der Betroffenen. FPA74 gilt nur für die US-amerikanische Bundesverwaltung und schützt nur die Rechte von „US persons“, d.h. Bürgern und rechtmäßigen Einwohnern der USA. Sofern US-Regierungen den Schutz durch Verwaltungsentscheidungen auf Ausländer ausgedehnt haben, konnte dies niemals die Möglichkeit einer gerichtlichen Überprüfung von Datenverarbeitungsvorgängen für Nicht-US-Residenten schaffen. Auch die verschiedenen Programme, wie etwa Safe Harbor oder Privacy Shield, mit denen die US-Regierungen versuchten Privatfirmen durch anscheinend angemessenen Datenschutz den freien Fluss von personenbezogenen Daten aus der EU zu ermöglichen, boten den Betroffenen keine Rechtsmittel. Lediglich im Rahmen des SWIFT-Datenaustausches wurde 2016 ein völkerrechtlicher Vertrag zwischen EU und USA geschlossen, in dem ausnahmsweise auch EU-Bürgern Zugang zu US-Gerichten zur Überprüfung sie betreffender Entscheidungen im Zusammenhang mit der Verarbeitung personenbezogener Daten gewährt wird.

Mit der DSGVO hat die Europäische Union zum einen festgelegt, dass die EU-Datenschutzregeln unabhängig vom Standort der Verantwortlichen anzuwenden sind, wenn personenbezogene Daten von Personen innerhalb der EU verarbeitet werden, wenn ihnen Dienste oder Produkte angeboten werden oder wenn ihr Verhalten innerhalb der EU überwacht wird. Zum anderen sollen die Sanktionen der DSGVO auch gegen Verantwortliche außerhalb der EU durchgesetzt werden. Allerdings haben sich die meisten großen ausländischen Unternehmen für die Errichtung von Niederlassungen in der EU entschieden, die dann in den Beschwerde- und Durchsetzungsverfahren als Verantwortliche gelten und ge-

gebenenfalls Adressaten der Maßnahmen der Aufsichtsbehörden sind.

Auch in den neuen Regelungen für den Digitalsektor, insbesondere dem Gesetz über Digitale Dienste (Digital Services Act, DSA), ist die Geltung der EU-Regeln auch für nicht in der EU ansässige Unternehmen vorgesehen, sofern sie in der EU tätig sind. Zum DSA haben sich das Europaparlament und der EU-Ministerrat auf eine Fassung geeinigt, der das Parlament bereits zugestimmt hat. Die Zustimmung der Mitgliedsstaaten wird erwartet. Die Verordnung soll spätestens 15 Monate nach ihrer Verabschiedung in Kraft treten. Ein Element des DSA ist die Festlegung der Verantwortlichkeiten von Plattformbetreibern, etwa sozialen Medien, bezüglich der durch sie veröffentlichten Inhalte, und damit das Bestreben freie Meinungsäußerung zu ermöglichen ohne Hasspropaganda freie Bahn zu gewähren.

Die Europäische Kommission erhofft sich durch die Digitalstrategie, die außer dem DSA u.a. auch das Gesetz über Digitale Märkte (Digital Markets Act, DMA) umfasst, sicherlich einen globalen Effekt zur Schaffung ähnlicher Regeln in anderen Wirtschaftsräumen. Ein solcher Effekt wird in Bezug auf die DS-GVO beobachtet, da bereits eine ganze Reihe von Staaten neue Datenschutzgesetze verabschiedet haben, die sich am Modell der DSGVO orientieren. Insgesamt wurden Mitte März 157 Staaten mit Datenschutzgesetzen gezählt[3]. Auch in den USA gibt es ein Gesetzgebungsverfahren für ein bundesweites umfassendes Datenschutzgesetz im Kongress, das bereits weiter fortgeschritten ist als alle vorherigen Versuche und das einige wesentliche Prinzipien des europäischen Datenschutzes in US-Recht einführen würde[4].

Entwicklung von Datenschutz und Privatheit im europäischen Recht

Rechtsprechung des EGMR und des EUGH

In der Rechtsprechung des EGMR wird Datenschutz im Wesentlichen als Aspekt des Menschenrechts auf Privatheit gemäß Artikel 8 der EMRK verstanden[5]. Dabei wird die Konvention 108, die die Prinzipien des Datenschutzes genauer festlegt, als Konkretisierung von Artikel 8 der EGMR zur Privatheit aufgefasst.

Dem EUGH steht mit Artikel 8 der EU Charta eine eigenständige Rechtsgrundlage zum Datenschutz zur Verfügung. Gleichzeitig enthält auch der eigentliche EU-Vertrag eine Bestimmung zum Datenschutz in Artikel 16 AEUV. Auf dieser Basis ist der Gerichtshof in der Lage das Grundrecht auf Datenschutz weiterzuentwickeln. Sowohl in der Charta als auch im Vertrag enthält die Bestimmung zum Datenschutz Elemente, die bisher bereits im sogenannten Sekundärrecht der EU, also den Richtlinien und Verordnungen, enthalten waren. Bieker[6] spricht hier von einem „reverse engineering"-Grundrecht. Von der Rechtsprechung des EUGH wäre auch eine Interpretation zu erwarten, wie die nur teilweise Übernahme der Datenschutzprinzipien im Charta-Artikel zu verstehen ist. Die Prinzipien der Fairness, der Zweckbestimmung, des notwendigen Rechtsgrundes für die Verarbeitung, des Auskunfts- und Berichtigungsrechtes und insbesondere die unabhängige Überwachung sind ausdrücklich wiedergegeben. Nicht ausdrücklich erwähnt sind hingegen solche Prinzipien wie Datensparsamkeit, zeitliche Begrenzung der Speicherung, Datensicherheit und die Nichtweitergabe außerhalb von Gebieten mit angemessenem Datenschutz. Diese Elemente sind natürlich weiterhin im Sekundärrecht, insbesondere in der DSGVO, der Richtlinie über den Datenschutz bei der Zusammenarbeit im Bereich Justiz und Inneres (LED) sowie in der Verordnung über den Datenschutz bei den Organen und Behörden der EU (EDPS-VO) festgelegt und werden auch in anderen Rechtsinstrumenten reflektiert, die als Rechtsgrundlage für die Verarbeitung personenbezogener Daten dienen.

Entwicklung des Digitalen Rechts der EU

Die Europäische Kommission hat eine umfangreiche Digitalstrategie[7] aufgesetzt, die auch zahlreiche Gesetzgebungsinitiativen umfasst. In den Gesetzgebungsprozessen zu DSA und DMA haben Rat und Parlament bereits informell Einigung erzielt. Die formelle Verabschiedung steht bevor. Weiterhin sind u.a. Gesetzgebungsverfahren zum AI Act, zum Data Act und zum europäischen Datenraum im Gange, deren Ergebnis auch Einfluss auf Grundrechte im Digitalen Raum haben wird.

Auf der anderen Seite stehen Gesetzgebungsverfahren, die direkt Grundrechte betreffen. Bereits seit 2017 liegt ein Entwurf für eine neue ePrivacy-Verordnung vor, die zum einen den Schutz der Privatsphäre bei der Kommunikation an die technische Entwicklung anpassen soll und zum anderen die Regelungen wieder mit dem europäischen Rechtsrahmen für elektronische Kommunikation in Einklang bringen soll, der insbesondere die Definition der betroffenen Dienste erweitert hat, so dass jetzt auch Messenger und andere nicht-traditionelle Kommunikationsdienste erfasst werden. Da die neuen Regelungen also auch für die umsatzstärksten Unternehmen der Digitalbranche gelten werden, ist der Lobbying-Druck außerordentlich stark und hat zu erheblicher Verzögerung durch den Widerstand im Ministerrat geführt. Im sogenannten informellen Trilog verhandeln Parlament, Rat und Kommission über den Vorschlag, ohne dass bisher eine Einigung erreicht wurde. Einigung erzielten die Gesetzgeber 2021 lediglich über eine Ausnahmeverordnung, die abweichend von den Pflichten der Kommunikationsdienstleister den Anbietern von Chat-Diensten weiterhin das Durchsuchen der Inhalte nach möglichen Anzeichen für Kindesmissbrauch erlaubt.

Die Bekämpfung von Kindesmissbrauch ist auch die Begründung für einen Legislativvorschlag für eine weitgehende Überwachung von Benutzernachrichten. Dieser Vorschlag wird zwar von Datenschutzbehörden und anderen Vertretern der Grundrechte abgelehnt, wird aber von der Kommission und vielen Regierungen der Mitgliedsstaaten weiter intensiv verfolgt.

Obwohl sie vom EUGH in mehreren Verfahren als grundrechtswidrig eingestuft wurde, wird die Vorratsdatenspeicherung von ihren Befürwortern immer wieder eingeführt, z. B. auch im Rahmen der ePrivacy-Verordnung.

Der zivilgesellschaftliche Widerstand gegen die Versuche zur Einschränkung von Grundrechten bleibt notwendig.

Eine besondere Herausforderung entsteht durch die militärische Konfrontation in Europa, durch die die Bedeutung der Cybersicherheit in der Politik erhöht wird. Damit wird auch der Ruf nach mehr Überwachungs- und Eingriffsmöglichkeiten im digitalen Raum lauter werden.

1 Selmayr, Martin: Einführung, in Ehmann/Selmayr (Hg.) DS-GVO Datenschutzgrundverordnung, Beck 2018.

2 Weichert, Thilo: Digitale Grundrechte im internationalen Kontext, in DANA 3/2022, S. 142 ff.

3 Greenleaf, Graham: Now 157 Countries: Twelve Data Privacy Laws in 2021/22 (March 15, 2022). (2022) 176 Privacy Laws & Business International Law Report 1, 3-8 UNSW Law Research, https://ssrn.com/abstract=4137418.

4 Zanfir-Fortuna, Gabriela: US vs. EU Privacy Reforms: A Comparison, in: Politico Digital Bridge, July, 7 2022, https://www.politico.eu/newsletter/digital-bridge/germanys-digital-void-transatlantic-privacy-what-to-do-about-web3/.

5 ECHR. Guide to the Case Law of the European Court of Human Rights – Data Protection, Council of Europe/European Court of Human Rights, 2022, https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf.

6 Bieker, Felix: The Right to Data Protection – Individual and Structural Dimensions of Data Protection in EU Law, Springer 2022.

7 Europäische Kommission, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_de.

Sabine Leutheusser-Schnarrenberger

Das Datenschutzgrundrecht – seit 40 Jahren unverzichtbar

Am 15. Dezember 1983 änderte sich in Deutschland die Welt der Grundrechte. Das Bundesverfassungsgericht schuf mit dem Volkszählungsurteil[1] das Grundrecht auf Datenschutz. Es war eine Zeitenwende.

Das Bundesverfassungsgericht hat mit dieser Entscheidung die grundsätzlichen Kernelemente des Rechts auf informationelle Selbstbestimmung entwickelt. Der Ausgangsfall erscheint rückblickend marginal. Die gesammelten Daten bezogen sich unter anderem auf Wohnungsgrößen, Regionen, aber auch auf eine zentral zu verwendende Personenkennziffer, die ihren Träger, also jeden Menschen in Deutschland, ein Stück gläserner machte.

Das Bundesverfassungsgericht hat mit der Grundsatzentscheidung zur Volkszählung 1983 unmissverständlich erklärt, dass zum allgemeinen Persönlichkeitsrecht das Recht des Einzelnen gehört selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte von ihm preisgegeben werden. Es hat die Gefahren gesehen, die dem Persönlichkeitsrecht unter den Vorzeichen der automatisierten Datenverarbeitung drohen, und reklamiert, dass der Einzelne davor besonders geschützt werden muss.

„Eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung, in der der Bürger nicht mehr wissen könne, wer was wann und bei welcher Gelegenheit über ihn weiß, ist mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar. Wer unsicher sei, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, werde versuchen, nicht durch solche Verhaltensweisen aufzufallen. ... Dies würde nicht nur die individuellen Entwicklungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung einer auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen, demokratischen Grundordnung sei. Hieraus folge: Freie Entfaltung der Persönlichkeit setze unter den modernen Bedingungen der Datenverarbeitung den Schutz des einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz sei daher von dem Grundrecht des Art. 2 Abs. 1 GG i.V. m. Art. 1 Abs. 1 GG umfasst."

Das Datenschutzrecht wird also aus der Unantastbarkeit der Menschenwürde abgeleitet, die alle staatliche Gewalt bindet und als objektive Wertordnung auch mittelbar Wirkung im Verhältnis der Bürger untereinander und im Verhältnis zu den Unternehmen entfaltet.[2] Das Grundrecht gewährleistet insoweit die Befugnis grundsätzlich selbst über die Preisgabe und Verwendung der persönlichen Daten zu bestimmen.[3]

Relevanz des informationellen Selbstbestimmungsrechts

Ist das eine vor bald 40 Jahren getroffene Entscheidung aus einer anderen Zeit ohne heutige Relevanz? Keinesfalls.

Damals haben die Richter vorausschauend geurteilt, auch wenn die Dynamik und Dimension der Digitalisierung nicht vorhersehbar war.

Die damals aufgestellten Anforderungen an Eingriffe in das Recht auf informationelle Selbstbestimmung sind heute genauso aktuell, vielleicht sogar noch bedeutsamer. Es geht um die grundgesetzlichen Freiheitsrechte, die die Grundlage unserer Demokratie darstellen und die durch technische Entwicklungen nicht ausgehöhlt werden dürfen. Ihnen liegt das Menschenbild des selbstbestimmten Individuums zu Grunde, das nicht Objekt, sondern Subjekt staatlichen und wirtschaftlichen Handels ist. Wenn manche IT-Firmen die Auffassung vertreten, das sei alles eine alte Idee, die Bedeutung der

Rechte der Bürgerin und des Bürgers aus der analogen Zeit hätten sich überholt, mit der neuen Technik wolle man eine neue Welt schaffen, die das Leben eines jeden Menschen erleichtern und lebenswerter machen würde und außerdem sei die neue digitale Welt nicht so schwerfällig und bürokratisch wie die demokratischen Abläufe, dann haben die Entwicklungen der letzten 20 Jahre diese Propaganda für ein Geschäftsmodell, das weitestgehend auf der massenhaften gewinnträchtigen Vermarktung personenbezogener Daten besteht, widerlegt.

Die rasante technologische IT–Entwicklung der Datenerfassung, -speicherung, -analyse und -verwendung brachte nicht nur viele Verbesserungen der Information und Kommunikation und auch neue wirtschaftliche Betätigungsfelder, sie ist auch mit einer disruptiven Wirkung für viele Geschäftsmodelle, ja für jeden Bereich des Lebens und Wirtschaftens verbunden. Und sie bietet mit den Unmengen an Datenerfassungen und -verknüpfungen, mit Big Data, mit selbstlernenden Algorithmen auf der Grundlage dieser Datenbasis nicht nur Möglichkeiten der verbesserten Prognose und natürlich der gezielten Werbung, sondern auch der personenbezogenen Profilbildung und der Überwachung des Verhaltens des Individuums. Es prägen also Chancen und Risiken diese Entwicklung. Risiken bestehen gerade hinsichtlich der Verletzung von Grundrechten.

Wenn wir nicht wollen, dass schleichend durch diese technologische Entwicklung die fundamentalen Werte ausgehöhlt werden, dann brauchen wir den richtigen Gestaltungsrahmen, um Freiheit im digitalen Zeitalter so leben zu können, dass die Rechte des Anderen wie sein Persönlichkeitsrecht, sein Recht auf Schutz der Privatsphäre und sein informationelles Selbstbestimmungsrecht vor unverhältnismäßigen Eingriffen geschützt werden.

Gefordert ist der nationale und europäische Gesetzgeber, aber als besondere „Schutzmacht" haben sich das Bundesverfassungsgericht und der Europäische Gerichtshof (EuGH) erwiesen. Sie haben den Datenschutz und Persönlichkeitsrechtsschutz mit ihrer Rechtsprechung weiterentwickelt.

Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Die Entscheidung des Bundesverfassungsgerichts zum Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ergänzt den Schutz der informationellen Selbstbestimmung. Das sog. IT-Grundrecht soll „den persönlichen und privaten Lebensbereich der Grundrechtsträger vor staatlichem Zugriff im Bereich der Informationstechnik auch insoweit bewahren, als auf das informationstechnische System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten".[4]

Als Hauptangriffspunkt sieht das Bundesverfassungsgericht den heimlichen Zugriff auf informationstechnische Dienste, die das Internet insgesamt, Rechnernetzwerke, Personal Computer, elektronische Geräte und natürlich Mobiltelefone umfassen. Offene Zugriffe sind aber nicht ausdrücklich ausgeschlossen. Es geht darum die Vertraulichkeits- und Integritätserwartung des Benutzers und der Benutzerin zu schützen, die immer dann betroffen ist, wenn Einblicke in wesentliche Teile der Lebensgestaltung erfolgen.[5] Heimlichkeit ist ein Intensitätskriterium.

Das Bundesverfassungsgericht ordnete Online-Durchsuchungen in einer späteren Entscheidung ausdrücklich als Eingriff in das genannte Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ein.[6] Eine Online-Durchsuchung ist ein tiefer Eingriff in das Persönlichkeitsrecht und das informationelle Selbstbestimmungsrecht, denn der Computer enthält nicht nur Texte, sondern macht das Kommunikationsverhalten des Nutzers transparent und erlaubt damit Einblicke in seine Gedanken, Vorstellungen, in den privaten Kern seiner Lebensgestaltung.

Deshalb dürfen Eingriffe nur unter gesteigerten Voraussetzungen insbesondere zum Schutz bedeutender Rechtsgüter zulässig sein. Tatsächliche Anhaltspunkte für eine im Einzelfall drohende konkrete Gefahr für ein überragend wichtiges Rechtsgut müssen vorliegen.[7] Entsprechende Maßnahmen sind demnach nur dann erlaubt, „wenn Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen und wenn erkennbar ist, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann. Ausreichend ist insoweit auch, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das individuelle Verhalten eines Betroffenen eine konkrete Wahrscheinlichkeit begründet, dass er solche Straftaten in überschaubarer Zukunft begehen wird."[8]

Eingriffe in dieses Recht sind nur auf Grund eines Gesetzes und unter Wahrung strenger Verhältnismäßigkeitsanforderungen zulässig.[9] Das Bundesverfassungsgericht verlangt zudem, dass in der gesetzlichen Grundlage bereits die Eingriffsschwelle definiert wird. Es unterscheidet dabei ausdrücklich nicht zwischen nachrichtendienstlichen und polizeilichen Eingriffsermächtigungen. Für beide Bereiche gelten daher gleich erhöhte Anforderungen an die Regelung des Eingriffsanlasses.[10]

Mit diesen hohen Anforderungen haben die Verfassungsrichterinnen und Verfassungsrichter dem Gesetzgeber einen engen Rahmen gesetzt, denn sie wissen aus leidvoller Erfahrung, dass sich die Sicherheitsinstitutionen nach ihren Vorstellungen eine möglichst weitgehende Eingriffsgrundlage wünschen, die für die tägliche Arbeit praktisch, aber nicht unbedingt grundrechtskonform ist. Sie wollen Daten zu verschiedenen Zwecken verwenden und möglichst leicht vernetzen können. Und die Verfassungsrichter wissen, dass der Gesetzgeber unter Berufung auf die innere Sicherheit diesen Vorstellungen gern Priorität einräumt nach dem Motto, das Bundesverfassungsgericht könne ja später seine Bedenken formulieren, jetzt sei erst einmal Handeln gefordert. Handeln, das auch die intensive Datennutzung zum Vorgehen gegen organisierte Kriminalität, Terrorismus und Extremismus erfordere. Gegen dieses Narrativ hat es der Datenschutz schwer. Er wird auf den Umgang mit personenbezo-

genen Daten als Information reduziert und das Persönlichkeitsrecht und informationelle Selbstbestimmungsrecht der Betroffenen als eigentliches Schutzgut des Datenschutzes werden nicht angemessen bewertet. Exemplarisch steht dafür die Antiterrordatei.

Antiterrordatei

Im Mittelpunkt des im Jahr 2006 in Kraft getretenen Antiterrordateigesetzes stand die Schaffung einer gemeinsamen Verbunddatei der Sicherheitsbehörden, die in ihrem Kern der Informationsanbahnung diente. Nachdem der Erste Senat des Bundesverfassungsgerichts mit Urteil vom 24. April 2013[11] mehrere Vorschriften des Gesetzes für unvereinbar mit dem Grundgesetz erklärt hatte, änderte der Bundesgesetzgeber die vom Bundesverfassungsgericht beanstandeten Vorschriften und ergänzte das Antiterrordateigesetz um die Vorschrift des § 6a ATDG („Erweiterte projektbezogene Datennutzung"). § 6a ATDG ermächtigt die Sicherheitsbehörden erstmalig zur so bezeichneten erweiterten Nutzung („Data-mining") von in der Antiterrordatei gespeicherten Datenarten, und zwar – über die Informationsanbahnung hinaus – auch zur operativen Aufgabenwahrnehmung. § 6a ATDG gestattet damit die unmittelbare Nutzung der Antiterrordatei auch zur Generierung neuer Erkenntnisse aus den Querverbindungen der gespeicherten Datensätze. Dies war bisher nur in Eilfällen möglich.

Diese Regelung stellt eine Grundrechtsverletzung dar. Verletzt wird das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG. Sie genügt nicht den besonderen verfassungsrechtlichen Anforderungen der hypothetischen Datenneuerhebung („informationelles Trennungsprinzip"). Aufgrund der gesteigerten Belastungswirkung einer erweiterten Nutzung einer Verbunddatei der Polizeibehörden und Nachrichtendienste muss diese dem Schutz von besonders gewichtigen Rechtsgütern dienen und auf der Grundlage präzise bestimmter und normenklarer Regelungen an hinreichende Eingriffsschwellen gebunden sein. Diesen Anforderungen genügt § 6a Abs. 2 Satz 1 ATDG nicht, während § 6a ATDG im Übrigen diesen Erfordernissen entspricht.[12] Die beiden Entscheidungen des Bundesverfassungsgerichts zur Antiterrordatei zeigen, dass der Gesetzgeber versucht jeden angeblichen verfassungsrechtlichen Spielraum zu nutzen.[13]

Die Formulierungen in den Entscheidungen ähneln stark den Ausführungen des Bundesverfassungsgerichts in seinen Entscheidungen zum IT-Grundrecht und zur Online-Durchsuchung. Da sich Zugriffe auf informationstechnische Systeme in aller Regel der Kenntnis der Betroffenen entziehen sind sie grundsätzlich unter den Vorbehalt einer richterlichen Anordnung zu stellen. Ausdrücklich führt das Bundesverfassungsgericht hierzu aus:

„Bewirkt eine heimliche Ermittlungsmaßnahme einen schwerwiegenden Grundrechtseingriff, so ist eine vorbeugende Kontrolle durch eine unabhängige Instanz verfassungsrechtlich geboten, weil der Betroffene sonst ungeschützt bliebe. Dem Gesetzgeber ist allerdings bei der Gestaltung der Kontrolle im Einzelnen, etwa bei der Entscheidung über die kontrollierende Stelle und das anzuwendende Verfahren, grundsätzlich ein Regelungsspielraum eingeräumt. Bei einem Grundrechtseingriff von besonders hohem Gewicht wie dem heimlichen Zugriff auf ein informationstechnisches System reduziert sich der Spielraum dahingehend, dass die Maßnahme grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen ist. Richter können aufgrund ihrer persönlichen und sachlichen Unabhängigkeit und ihrer ausschließlichen Bindung an das Gesetz die Rechte des Betroffenen im Einzelfall am besten und sichersten wahren […]."[14]

Zum Schutz des Kernbereichs privater Lebensgestaltung sind besondere Vorkehrungen geboten. Dieser ergibt sich unmittelbar aus dem unantastbaren Schutz der Menschenwürde. Zu diesem fordert die verfassungsgerichtliche Rechtsprechung, dass bei „heimlichen Überwachungsmaßnahmen staatlicher Stellen … selbst überwiegende Interessen der Allgemeinheit einen Eingriff in ihn nicht rechtfertigen können […]. Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art ohne die Angst zum Ausdruck zu bringen, dass staatliche Stellen dies überwachen […]."[15]

Deshalb soll eine Informationserhebung aus diesem Bereich möglichst unterbleiben.[16] Ist dies nicht möglich, muss der Gesetzgeber Sicherungen auf der Aus- und Verwertungsebene vorsehen. Hierzu muss insbesondere sichergestellt werden, dass erhobene Daten mit Kernbereichsbezug unverzüglich gelöscht werden und eine Verwertung ausgeschlossen ist.[17]

Diese verfassungsgerichtlichen Ausprägungen des Datenschutzrechts haben dessen Schutzwirkung seit 1983 erweitert und sind fester Bestandteil des Grundrechtsschutzes.

Die anlasslose Vorratsdatenspeicherung

Die Spuren des Grundrechts auf Datenschutz seit 1983 sind also tief, aber längst nicht unumstritten. Dies zeigt sich in der unendlichen Geschichte der anlasslosen Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten (VDS), die den deutschen und europäischen Gesetzgeber, die Verfassungsgerichte mehrerer Mitgliedstaaten und den EuGH immer wieder bis zum heutigen Tag beschäftigen.

Der Gerichtshof der Europäischen Union (EuGH) ist seit einigen Jahren mit seinen Entscheidungen zu einem Verteidiger und Garant der Grundrechte der Bürgerinnen und Bürger in der Europäischen Union geworden. Der anlasslosen Vorratsdatenspeicherung hat er mit seinen beiden Urteilen im Jahr 2014[18] und 2016[19] einen deutlichen Riegel vorgeschoben und den Mitgliedstaaten der Europäischen Union (EU) die rote Karte gezeigt. Eigentlich sollte damit die unendliche Geschichte der flächendeckenden, anlasslosen Speicherung von Telekommunikationsverbindungsdaten, die mit Verabschiedung der Richtlinie 2006/24/EG am 15.03.2006 begann, endlich und endgültig beendet sein.[20] Denn der EuGH hat unmissverständlich die ohne jeden Anlass und ohne eine Beschränkung auf einen bestimmten

Personenkreis gesetzlich erlaubte Datenspeicherung für ungültig und nichtig erklärt, da sie gegen Art. 7 und Art. 8 der Grundrechtecharta der EU (GRCh) verstößt und den Verhältnismäßigkeitsgrundsatz nach Art. 52 Abs.1 der GRCh verletzt.

Beschränkungen des Rechtes auf Privatheit und des Schutzes der personenbezogenen Daten können danach nur dann für zulässig erachtet werden, wenn sie auf das absolut notwendige Maß begrenzt sind.[21] Das ist bei der unbegrenzten Speicherung der Daten von Personen, die keinen unmittelbaren oder noch nicht einmal einen mittelbaren Bezug zu einer Handlung haben, die zur Strafverfolgung Anlass gibt, nicht anzunehmen. Diese Massenspeicherungen sind nicht das absolut notwendige Instrument, denn es kann als Alternative die durch konkrete Anhaltspunkte begründete Speicherung von Daten einzelner Personen geben. Außerdem gibt es noch nicht einmal eine Ausnahme für die Personen, deren Kommunikationsvorgänge nach den nationalen Vorschriften dem Berufsgeheimnis unterliegen. Das alles hat die Gesetzgeber der Mitgliedstaaten nicht davon abgehalten an einer teilweise etwas eingeschränkten, aber anlasslosen Vorratsdatenspeicherung festzuhalten, weil diese die Vertraulichkeit der Kommunikation gefährdende Überwachungsmaßnahme angeblich unverzichtbar zum Vorgehen gegen die organisierte Kriminalität und Terroristen sei. Alle Zweifelsfragen gegen die Vorratsdatenspeicherung bis hin zu der Behauptung, die nationalen Gesetze fielen nicht in die Zuständigkeit des Unionsrechts[22], wurden mit dem Urteil des EuGH vom 21.12.2016 ausgeräumt. Es betraf die nationalen Gesetze in Schweden und im Vereinigten Königreich, die mittels zweier Vorabentscheidungsersuchen dem EuGH vorgelegt wurden. Der EuGH bestätigte auch für die VDS-Gesetze der anderen Mitgliedstaaten noch einmal die Anforderung, dass diese die Grundrechtseingriffe auf das „absolut Notwendige“ zu begrenzen haben. Dies sei bei einer nationalen Regelung nicht gegeben, die „die allgemeine und unterschiedslose Vorratsdatenspeicherung sämtlicher Verkehrs- und Standortdaten vorsieht,“ weil sie die Vorratsdatenspeicherung zur Regel macht, obwohl sie die „Ausnahme zu sein hat“.[23] An dieser Entscheidung wird sich auch das deutsche „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10.12.2015[24]“ zu messen haben, das am 18.12.2015 in Kraft trat. Obwohl diese umbenannte Vorratsdatenspeicherung vielen Anforderungen des Bundesverfassungsgerichts und des EuGH in seinem Urteil zu Digital Rights in Detailregelungen Rechnung zu tragen sucht, bleibt es bei dem Mangel, dass alle Nutzer anlasslos erfasst werden. Die konsequente Rechtsprechung des EuGH zu diesem Thema ist beeindruckend.

Er hat wiederholt (z.B. Tele2 Sverige und Watson[25], Ministerio Fiscal[26]) festgestellt, dass eine präventive, allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten mit europäischem Recht nicht vereinbar ist. Zuletzt wurde diese Rechtsprechung im Urteil La Quadrature du Net u.a. vom 6. Oktober 2020[27] umfassend gewürdigt, zusammengefasst und bestätigt. Das aktuellste Urteil vom 5. April 2022[28], mit dem die irischen Regelungen zur anlasslosen Vorratsdatenspeicherung gekippt wurden, bezieht sich auf diese gefestigte Rechtsprechung und setzt sie fort. Das noch anhängige Vorlageverfahren des BVerwG zu den ausgesetzten deutschen Bestimmungen zur anlasslosen Vorratsdatenspeicherung (SpaceNet und Telekom Deutschland[29]) lässt keine Abweichung von der ständigen Rechtsprechung erwarten. In seinen Schlussanträgen[30] vom 18. November 2021 weist der Generalanwalt Manuel Campos Sanchéz-Bordona ausdrücklich darauf hin, dass sich seiner Ansicht nach die Unvereinbarkeit der deutschen Regelungen für eine anlasslose, flächendeckende und personell, zeitlich und geografisch undifferenzierte Vorratsdatenspeicherung von Telekommunikations-Verkehrsdaten mit europäischem Recht schon aus der bisherigen Rechtsprechung des EuGH ergibt.

Fazit

Das Grundrecht auf Datenschutz erfreut sich großer Vitalität und hat seit 1983 zu einer Zeitenwende geführt. Zeitenwende in dem Sinn, dass die informationelle Selbstbestimmung als Teil des Persönlichkeitsrechtschutzes grundlegend die Gesetzgebung prägt und zur Verabschiedung der europäischen Datenschutz-Grundverordnung geführt hat. Trotz kontroverser Positionen hat sie sich in bald fünfjähriger Anwendung (2023) bewährt. Es ist eine Zeitenwende, dass das Machtverhältnis zwischen der häufig marktdominanten Stellung der Internetgiganten einerseits und der negativen Freiheit in Ruhe gelassen zu werden[31] sowie der positiven Freiheit Datenschutz- und Persönlichkeitsrechte zu leben, neu justiert wurde, auch wenn die konsequente Durchsetzung aufwändig und schwierig ist.

Keine Zeitenwende hat es an manchen grundsätzlichen Einstellungen zum Datenschutz gegeben. Nach wie vor stehen sich Täter- versus Opferschutz, wirtschaftlicher Hemmschuh oder Wettbewerbsvorteil gegenüber. Deshalb muss es weiter gehen. Max Schrems hat mit dem Safe-Harbour-Urteil des EuGH einen wichtigen Schritt zum datenschutzkonformen Transfer von Daten zwischen Unternehmen der EU und den USA initiiert. Nach dem gerichtlichen Scheitern des Nachfolgers Privacy Shield müssen endlich mit Privacy Shield 2.0. die EuGH Vorgaben ernst genommen und umgesetzt werden. Ein jahrelanger Datenschutz-Lernprozess fände seinen Abschluss.

Es geht um viel. Es geht grundsätzlich darum, wie selbstbestimmt wir angesichts der technischen digitalen Entwicklungen leben können und leben wollen. Datenschutz ernst nehmen muss unter anderem auch zu mehr Transparenz der Wirkungsweise der Algorithmen führen. Aber am wichtigsten ist, dass wir als Datenträgerin und Datenträger wissend und selbstbewusst mit unserer informationellen Selbstbestimmung umgehen und Datenmissbrauch entgegentreten. Die Grundlage schuf das Volkszählungsurteil von 1983.

1 BVerfGE vom 15. Dezember 1983 – 1 BvR 209/82.

2 Lüth – Urteil des BVerfG.

3 BVerfG 65, 1 - 71.

4 BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, juris Rn. 201.

5 BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07, Rn 203.

6 BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, juris Rn. 210.

7 BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, juris Rn. 212; BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, juris Rn. 242.

8 BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, juris Rn. 213; ähnlich: BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, juris Rn. 251.

9 BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, juris Rn. 212.

10 BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, juris Rn. 254 ff.

11 BVerfG 1 BvR 1215/07 - BVerfG E 133, 277 ff.

12 Pressemitteilung des Bundesverfassungsgerichts Nr. 104/2020 vom 11. Dezember 2020.

13 Beschluss des BVerfG vom 10. November 2020 – 1 BvR 3214/15.

14 BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07, juris Rn. 259.

15 BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07, juris Rn. 271.

16 BVerfG, Urteil vom 20. September 2016, 1 BvR 5/13, juris Rn. 219.

17 Siehe dazu wissenschaftlicher Dienst des Bundestages, Ausarbeitung, WD 3-3000-088/19, Seite 6 ff.

18 EuGH vom 8.4.2014, NJW 2014, 2169 ff.

19 EuGh vom 21.12.2016, NJW 2017, 717 ff.

20 zur Diskussion dazu Leutheusser-Schnarrenberger, ZRP 2007, 9 ff.

21 EuGH Urteil des Gerichtshofs in den verbundenen Rechtssachen C-293/12 und C-594/12 vom 8. April 2014, Rdn. 65.

22 Prof. Dr. Roßnagel, Vorratsdatenspeicherung rechtlich vor dem Aus?, NJW 2017, 696 ff.

23 EuGH – Entscheidung, aaO, Rdn 103f, Roßnagel, aaO, 697.

24 BGBL I 2015, 2218 f.

25 Urteil des EuGH vom 21. Dezember 2016 in den verbundenen Rechtssachen C203/15 und C698/15 „Tele2 Sverige und Watson".

26 Urteil des EuGH vom 2. Oktober 2018 in der Rechtssache C 207/16 „Ministerio Fiscal".

27 Urteil des EuGH vom 6. Oktober 2020 in den verbundenen Rechtssachen C-511/18, C-512/18 und C-520/18 „La Quadrature du Net u.a.".

28 Urteil des EuGH vom 5. April 2022 in der Rechtssache C-140/20 „Commissioner of the Garda Síochána u.a.".

29 Verbundene Rechtssachen C-793/19 (SpaceNet AG) und C-794/19 (Telekom Deutschland GmbH).

30 Schlussanträge des Generalanwalts Manuel Campos Sanchéz-Bordona vom 18. November 2021, verbundene Rechtssachen C-793/19 und C-794/19.

31 Frank Schirrmacher in einem Beitrag der ARD am 30.3.2014, Fundstelle siehe Yvonne Hofstetter, aaO, Seite 285.

Steffen Pau

Das kirchliche Datenschutzrecht

Die Europäische Datenschutz-Grundverordnung (DSGVO) sieht für zwei grundrechtlich geschützte Bereiche – Medien und Kirchen bzw. Religionsgemeinschaften – Ausnahmen für ihre Anwendbarkeit vor. Art. 85 DSGVO ermöglicht es den Mitgliedsstaaten für die Bereiche der Freiheit der Meinungsäußerung und der Informationsfreiheit die Verarbeitung personenbezogener Daten für journalistische und andere dort genannte privilegierte Zwecke abweichende Regelungen zu treffen und für diese Bereiche auch eigene Aufsichtsstrukturen vorzusehen. Der zweite in der DSGVO besonders geregelte Bereich ist der Datenschutz der Kirchen und Religionsgemeinschaften in Art. 91 DSGVO.[1]

Verfassungs- und primärrechtliche Grundlagen

Das deutsche Grundgesetz schützt in Art. 4 GG die Religionsfreiheit. Inhalte dieses Grundrechts haben in Art. 10 Abs. 1 GRCh ihren Eingang in die Charta der Grundrechte der Europäischen Union gefunden.

Ergänzt wird der Schutz der Religionsfreiheit aus Art. 4 GG in Deutschland durch Art. 140 GG, der die Bestimmungen der Regelungen der Art. 136 bis 139 und 141 der Weimarer Reichsverfassung (WRV) in das Grundgesetz überführt. Dadurch wird eine korporative Seite der verfassungsrechtlichen Gewährleistung von Religionsfreiheit im Grundgesetz implementiert,[2] die es den Religionsgemeinschaften unter anderem ermöglicht, ihre Angelegenheiten selbstständig innerhalb der Schranken der für alle geltenden Gesetze zu ordnen und zu verwalten (Art. 140 GG i.V.m. Art. 137 Abs. 3 WRV).

Die DSGVO nimmt diese Rahmenbedingungen auf Grund von Art. 17 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) auf und setzt sie im Art. 91 DSGVO um. Art. 91 DSGVO ermöglicht den Kirchen bestehende eigene datenschutzrechtliche Regelungen weiter anzuwenden, sofern diese mit den Regelungen der DSGVO in Einklang gebracht werden. Ebenso eröffnet Art. 91 DSGVO die Möglichkeit eine eigene Datenschutzaufsicht zu installieren, die die Vorgaben des Kapitels VI der DSGVO erfüllen muss. Damit beachtet diese Regelung das Recht des Einzelnen auf den Schutz der personenbezogenen Daten und gleichermaßen den Status der Religionsgesellschaften nach Art. 140 GG i.V.m. Art. 137 Abs. 3 WRV (korporative Religionsfreiheit).[3]

Der europäische Gesetzgeber ermöglicht es der Kirche durch die Regelung des Art. 91 DSGVO die nationalen staatskirchenrechtlichen Spielräume trotz der zentralen europäischen Gesetzesvorgabe weiter beizubehalten. Damit kommt der europäische Gesetzgeber den Vorgaben nach, die im Art. 17 AEUV festgeschrieben wurden. Nach dieser Vorschrift achtet die Europäische Union den Status, den Kirchen, religiöse Ver-

einigungen oder Gemeinschaften in den Mitgliedsstaaten nach deren Rechtsvorschriften genießen, und beeinträchtigt diesen Status nicht (Art. 17 Abs. 1 AEUV). Die Vorschrift trägt der Tatsache Rechnung, dass das europäische Recht immer stärkere Auswirkungen auf die Kirchen hat und diese gerade in ihrem „Proprium" berühren kann.[4]

Art. 91 DSGVO gibt damit sowohl den Rahmen für das aktuelle Gesetz über den Kirchlichen Datenschutz (KDG) vor, als auch für die Einrichtung eigener Datenschutzaufsichten der katholischen Kirche.

Artikel 91 DSGVO als Ausgangspunkt des heutigen kirchlichen Datenschutzes

Art. 91 Abs. 1 DSGVO sieht vor, dass eine Kirche oder eine religiöse Vereinigung oder Gemeinschaft, die in einem Mitgliedstaat umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung von deren Daten zum Zeitpunkt des Inkrafttretens der DSGVO anwendet, diese Regeln weiter anwenden darf, sofern diese Regeln mit der DSGVO in Einklang gebracht werden.

Diese Voraussetzungen treffen auf die datenschutzrechtlichen Regelungen der katholischen Kirche in Deutschland zu.[5]

Die deutschen (Erz-)Diözesen hatten schon Ende der 70er-Jahre mit der „Anordnung über den kirchlichen Datenschutz (KDO)" eigene kirchliche Datenschutzgesetze geschaffen.[6] Damit können sie auf eine vergleichbar lange Anwendung datenschutzrechtlicher Regelungen zurückblicken wie der Gesetzgeber des Bundesdatenschutzgesetzes.

Das kirchliche Datenschutzrecht sowohl in der katholischen Kirche als auch das Datenschutzgesetz der Evangelischen Kirche in Deutschland (EKD) wurden im Laufe der Jahre immer wieder an die Entwicklungen des Bundesdatenschutzgesetzes angepasst. Daher konnten die katholische Kirche und die EKD zum Inkrafttreten der DSGVO im Mai 2016 auf umfassende Regelungen zurückgreifen.[7]

Sowohl die katholische als auch die evangelische Kirche haben vor Mai 2018 auch den notwendigen Anpassungsbedarf der im Jahr 2016 bestehenden eigenen datenschutzrechtlichen Regelungen erfasst und ihre jeweiligen Gesetze angepasst, so dass auch die Forderung des Art. 91 Abs. 1 DSGVO erfüllt wurde, dass die Regelungen mit der DSGVO in Einklang gebracht werden müssen.[8]

Das Gesetz über den kirchlichen Datenschutz (KDG)

In der katholischen Kirche liegt die Gesetzgebungsgewalt für kirchliche Gesetze grundsätzlich bei den einzelnen (Erz-)Bischöfen für ihre jeweiligen (Erz-)Diözesen.[9] Für Regelungen, die für die Kirche in allen Ländern gelten sollen, liegt die Gesetzgebung beim Heiligen Stuhl in Rom.

Das Gesetz über den kirchlichen Datenschutz (KDG) wurde daher von den 27 Diözesanbischöfen für ihre jeweilige (Erz-)Diözese als Gesetz in Kraft gesetzt und in den entsprechenden kirchlichen Amtsblättern veröffentlicht. Dies geschah auf Basis einer vom Verband der Diözesen Deutschlands – dem Rechtsträger der Deutschen Bischofskonferenz – erarbeiteten Musterfassung, um eine einheitliche Umsetzung der datenschutzrechtlichen Regelungen zu erreichen.[10] Ergänzend zum KDG wurde auch noch eine Durchführungsverordnung (KDG-DVO) von den einzelnen (Erz-)Diözesen erlassen, die konkretisierende Ausführungen zum KDG enthält.[11]

Ein Blick in das Inhaltsverzeichnis des KDG (wie auch des DSG-EKD) zeigt, dass das Gesetz etwas kürzer ausfällt als die DSGVO. Hier hat der kirchliche Gesetzgeber die Teile der DSGVO nicht übernommen, die für seinen Regelungsbereich nicht einschlägig waren. So fehlt beispielsweise das Kapitel über den Europäischen Datenschutzausschuss und die Zusammenarbeit der Datenschutzaufsichten auf europäischer Ebene, da dies nicht vom kirchlichen Gesetzgeber – auch nicht im Sinne des In-Einklangbringens – zu regeln war.

Ein zweiter Blick auf das kirchliche Gesetz zeigt eine von der DSGVO vertraute Gliederung des Gesetzes und viele Regelungen, die inhaltsgleich aus der DSGVO übernommen wurden. Hier zeigen sich für den Rechtsanwender die Vorteile des Einklangs der kirchlichen Regelungen mit der DSGVO. Der Rechtsanwender findet viele vertraute Regelungen und kann so auch die Kommentarliteratur zur DSGVO an vielen Stellen verwenden.[12] Ebenso fällt bei einem Blick in das Gesetz auf, dass der kirchliche Gesetzgeber auch die Umsetzung der europarechtlichen Vorgaben der DSGVO in das nationale Datenschutzrecht, namentlich die Neufassung des Bundesdatenschutzgesetzes, mit in den Blick genommen hat. Daher sind im kirchlichen Gesetz auch Fragmente von Regelungen des neuen Bundesdatenschutzgesetzes zu finden.

Da die Vorgabe des Art. 91 DSGVO aber gerade nicht war die DSGVO eins-zu-eins zu übernehmen, gibt es auch Unterschiede zur DSGVO, die vor dem Hintergrund kirchlicher Besonderheiten in das Gesetz eingefügt wurden.

Dabei gibt es Vorschriften, bei denen der Grund für die kirchenspezifische Regelung sofort ersichtlich ist, wie z.B. die Regelung des § 2 Abs. 3 KDG, die daran erinnert, dass die Wahrung des Beicht- und Seelsorgegeheimnisses und anderer dort genannter Verschwiegenheitspflichten unberührt bleiben oder des § 14 KDG-DVO, der ergänzend den Umgang mit personenbezogenen Daten, die dem Beicht- oder Seelsorgegeheimnis unterliegen, regelt. Auch bei der Begriffsdefinition der „besonderen Kategorien personenbezogener Daten" in § 4 Nr. 2 KDG wird so ein Unterschied deutlich. Die Zugehörigkeit zu einer Kirche oder Religionsgemeinschaft fällt nicht in die Gruppe der besonderen Kategorien personenbezogener Daten im kirchlichen Datenschutzgesetz (vgl. § 4 Nr. 2 Satz 2 KDG), da dies ein Datum ist, welches bei vielen Verarbeitungen personenbezogener Daten im kirchlichen Bereich zwangsläufig anfällt (z.B. Eintragung in das Taufregister).

Bei anderen Vorschriften mag die kirchliche Besonderheit für eine Abweichung vom Wortlaut der DSGVO nicht immer sofort ersichtlich sein. Hier wurden teilweise Regelungsinhalte aus dem Vorgängergesetz, der Anordnung über den kirchlichen Datenschutz (KDO), übernommen oder versucht – im Rahmen des durch die DSGVO Möglichen – eigene Akzente zu setzen oder sprachliche Anpassungen vorzunehmen.

So erscheint das KDG bei der Einwilligung mit seinem Schriftformerfordernis in § 8 Abs. 2 Satz 1 KDG strenger als die DSGVO, die in Art. 7 Abs. 1 DSGVO vorgibt, dass der Verantwortliche die

Einwilligung nachweisen können muss. Inwieweit hier in der Praxis im täglichen Umgang mit der Einwilligung wirklich große Unterschiede bestehen, ist bei vielen Sachverhalten fraglich, da einerseits § 8 Abs. 2 Satz 1 KDG als Ausnahme von dem Schriftformerfordernis selbst „eine andere Form" der Einwilligung auf Grund besonderer Umstände vorsieht und andererseits die Nachweispflicht der DSGVO in vielen Fällen auch zu einer textlichen oder schriftlichen Fassung der Einwilligung führt.

Anwendungsbereich des KDG

In den Anwendungsbereich des KDG sind durch § 3 KDG alle kirchlichen Stellen einbezogen, unabhängig davon, ob es sich um verfasst kirchliche Stellen (z.B. die Diözesen oder die Kirchengemeinden) oder um Einrichtungen der Caritas handelt. Auch kirchliche Körperschaften, Stiftungen, Anstalten, Werke, Einrichtungen und sonstige kirchliche Rechtsträger ohne Rücksicht auf ihre Rechtsform sind vom Anwendungsbereich umfasst. Damit wird deutlich, dass alle kirchlichen Einrichtungen, nicht nur der kirchliche „Kernbereich" der verfassten Kirche, in den Anwendungsbereich des KDG fallen. Daher gehören auch kirchliche Krankenhäuser, kirchliche Pflegeeinrichtungen, kirchliche Schulen oder kirchliche Kindertagesstätten zu den Stellen, die das KDG anwenden.

Betriebliche Datenschutzbeauftragte

Für den Bereich der verfassten Kirche (also die (Erz-)Diözesen und die Pfarreien bzw. deren Zusammenschlüsse auf der mittleren Verwaltungsebene) sind nach dem KDG zwingend betriebliche Datenschutzbeauftragte zu benennen (vgl. § 36 Abs. 1 KDG). Die anderen kirchlichen Stellen haben einen solchen gemäß § 36 Abs. 2 KDG zu benennen, wenn entweder mehr als zehn Personen[13] ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind oder die Kerntätigkeit des Verantwortlichen in der Durchführung von Verarbeitungsvorgängen besteht, die eine umfangreiche regelmäßige und systematische Überwachung der betroffenen Personen erfordern oder die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten gemäß § 12 KDG besteht.

Die betrieblichen Datenschützer unterstützen die Leitungen der Einrichtungen bei der Erfüllung ihrer Pflichten zur Beachtung datenschutzrechtlicher Vorgaben und wirken auf deren Einhaltung hin. Damit die Datenschutzbeauftragten ihre Aufgaben erfüllen können sind sie in die betrieblichen Prozesse und Informationsflüsse einzubinden. Der betriebliche Datenschutzbeauftragte genießt Kündigungsschutz nach § 37 Abs. 4 KDG, soweit keine außerordentliche Kündigung in Betracht kommt.

Kirchliche Datenschutzaufsichten

Durch die umfassenden eigenen datenschutzrechtlichen Regelungen des KDG und des DSG-EKD im Einklang mit Art. 91 Abs. 1 DSGVO haben beide Kirchen auch die Möglichkeit gemäß Art. 91 Abs. 2 DSGVO eigene kirchliche Datenschutzaufsichten einzurichten. Auf katholischer Seite sind in den einzelnen (Erz-)Diözesen die Diözesandatenschutzbeauftragten als Leitungen der Datenschutzaufsichten bestellt worden (§§ 42 ff. KDG). Jeweils mehrere (Erz-)Diözesen haben von der Möglichkeit Gebrauch gemacht die Diözesandatenschutzbeauftragten als Datenschutzaufsicht auch für mehrere (Erz-) Diözesen zu bestellen. So haben beispielsweise die nordrhein-westfälischen (Erz-)Diözesen mit dem Katholischen Datenschutzzentrum als Körperschaft des öffentlichen Rechts und dem gemeinsamen Diözesandatenschutzbeauftragten eine gemeinsame Datenschutzaufsicht bestellt.[14]

So wie das kirchliche Datenschutzrecht unter den Voraussetzungen von Art. 91 Abs. 1 DSGVO die Anwendung der DSGVO verdrängt, so treten die kirchlichen Datenschutzaufsichten unter den Voraussetzungen des Art. 91 Abs. 2 DSGVO an die Stelle der Landesdatenschutzbeauftragten für die kirchlichen Einrichtungen, die dem kirchlichen Datenschutz unterfallen. Dabei nehmen sie – ebenso wie die Landesdatenschützer – die breite Aufgabenpalette einer Datenschutzaufsicht wahr. Da alle deutschen (Erz-)Diözesen die Möglichkeit genutzt haben eine eigene Datenschutzaufsicht zu installieren, sind die Diözesandatenschutzbeauftragten die zuständigen Aufsichten, wenn es zum Beispiel um datenschutzrechtliche Beschwerden gegen kirchliche Einrichtungen geht.

Um eine möglichst einheitliche Auslegung der kirchlichen Regelungen zum Datenschutz durch die kirchlichen Aufsichten zu erreichen, stimmen sich die Diözesandatenschutzbeauftragten in der Konferenz der Diözesandatenschutzbeauftragten in zentralen Fragen ab, fassen gemeinsame Beschlüsse und formulieren gemeinsame Standpunkte.[15] Daneben besteht ein enger Austausch mit den Datenschutzaufsichten der evangelischen Kirche und den staatlichen Datenschutzaufsichtsbehörden.

Kirchliche Datenschutzgerichte

Die DSGVO sieht vor, dass sowohl gegen Entscheidungen der Datenschutzaufsicht, als auch gegen die Verantwortlichen bzw. Auftragsverarbeiter direkt, wirksame gerichtliche Rechtsbehelfe bestehen müssen (vgl. Art. 78, 79 DSGVO). Diese Vorgabe ist mit § 49 KDG bzw. § 47 DSG-EKD in kirchliches Recht umgesetzt worden.[16]

Im außerkirchlichen Bereich sind für diese gerichtlichen Rechtsbehelfe gemäß der DSGVO die Verwaltungsgerichte zuständig. Im Geltungsbereich des DSG-EKD werden diese Streitigkeiten den kirchlichen Verwaltungsgerichten der EKD zugewiesen (vgl. § 47 DSG-EKD).

Da eine kirchliche Verwaltungsgerichtsbarkeit im Bereich der Deutschen Bischofskonferenz nicht besteht, hat die Deutsche Bischofskonferenz parallel zur Inkraftsetzung des KDG eine Gerichtsordnung für ein kirchliches Gericht speziell für diese Streitigkeiten erlassen.

In der Kirchlichen Datenschutzgerichtsordnung (KDSGO) wird die Errichtung kirchlicher Gerichte speziell für Streitigkeiten aus § 49 KDG geregelt. Die KDSGO sieht dabei zwei Instanzen vor. In der ersten Instanz entscheidet das Interdiözesane Datenschutzgericht (IDSG). Gegen die Entscheidungen des IDSG kann dann die Entscheidung des Datenschutzgerichts der Deutschen Bischofskonferenz (DSG-DBK) beantragt werden.

Als Richter konnten für beide Instanzen Professoren, Richter und andere Expertinnen und Experten mit langjähriger Erfahrung im Datenschutz gewonnen werden, die eine hohe Qualität der Arbeit des Gerichtes sicherstellen. Entscheidungen der Gerichte werden teilweise auf der Seite der Deutschen Bischofskonferenz veröffentlicht.[17]

Fazit

Die katholische Kirche in Deutschland hat – ebenso wie die Evangelische Kirche in Deutschland – die Anforderungen des Art. 91 DSGVO mit der Neufassung des kirchlichen Datenschutzgesetzes vor dem 25. Mai 2018 erfüllt und dazu eigene Datenschutzaufsichten eingerichtet, die die in Kapitel VI der DSGVO niedergelegten Bedingungen erfüllen. Die gerichtliche Überprüfung erfolgt durch die speziell dafür auf Ebene der Deutschen Bischofkonferenz eingerichteten Gerichte in Datenschutzangelegenheiten.

1 Der Beitrag betrachtet die von den (Erz-)Diözesen in Deutschland jeweils auf Basis des Musterentwurfes des Gesetzes über den Kirchlichen Datenschutz (KDG) in der Fassung des einstimmigen Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 20. November 2017 in Kraft gesetzten Datenschutzgesetze. Diese Betrachtung wird ergänzt um Verweise auf das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz – DSG-EKD) vom 15. November 2017. Datenschutzrechtliche Regelungen anderer Kirchen oder Religionsgemeinschaften in Deutschland oder in anderen europäischen Ländern konnten in diesem Beitrag nicht betrachtet werden. Hinweise auf weitere kirchliche Datenschutzgesetze (ohne Anspruch auf Vollständigkeit) sammelt beispielsweise Felix Neumann in seinem Blog: https://artikel91.eu/rechtssammlung/.

2 Siehe hierzu auch Hense, Art. 91 Datenschutz-Grundverordnung und das kirchliche Selbstbestimmungsrecht, in: Pau (Hrsg.), Kirchlicher Datenschutz – gewachsener Baustein kirchlicher Selbstverwaltung, Katholisches Datenschutzzentrum, Dortmund 2021, S. 35 ff. (online abrufbar).

3 Hense in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 91, Rn. 1 mit weiteren Erläuterungen.

4 Vgl. dazu Streinz in: Streinz, EUV/AEUV, 3. Aufl. 2018, Art. 17 AEUV, Rn. 7 ff. und 12.

5 Dies gilt ebenso für die Regelungen der EKD zum Datenschutz.

6 Zur Entwicklung des kirchlichen Datenschutzrechts vgl. Pau, Kirchlicher Datenschutz von den Anfängen bis zum KDG, in: Pau (Hrsg.), Kirchlicher Datenschutz – gewachsener Baustein kirchlicher Selbstverwaltung, Katholisches Datenschutzzentrum, Dortmund 2021, S. 51 ff. (online abrufbar). Das Datenschutzgesetz der EKD hat eine vergleichbare Entwicklung genommen.

7 Hense in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 91, Rn. 19; Jacob in: Auernhammer, DSGVO BDSG, 7. Aufl. 2020, Art. 91, Rn. 12.

8 Herbst in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, Art. 91, Rn. 15a; Jacob in: Auernhammer, DSGVO BDSG, 7. Aufl. 2020, Art. 91 Rn. 13.

9 Auf einige Besonderheiten – z.B. für die Ordensgemeinschaften päpstlichen Rechts – wird hier nicht näher eingegangen.

10 Die Musterfassung ist abrufbar als Teil der Arbeitshilfe Nr. 320 auf der Seite https://www.dbk.de/themen/kirche-staat-und-recht/datenschutz-faq der Deutschen Bischofskonferenz. In der Arbeitshilfe ist auch eine Übersicht der Fundstellen der Veröffentlichungen des KDG in den Amtsblättern der (Erz-)Diözesen enthalten.

11 Der Mustertext der KDG-DVO ist ebenfalls in der Arbeitshilfe Nr. 320 der Deutschen Bischofskonferenz (siehe En. 10) enthalten.

12 Für das KDG liegt auch eine eigene Kommentierung vor: Sydow, Kirchliches Datenschutzrecht, Baden-Baden 2021. Für das DSG-EKD ist eine Kommentierung in Vorbereitung.

13 Der kirchliche Gesetzgeber hat die Änderung des § 38 Abs. 1 BDSG mit der Anhebung der Schwelle zur verpflichtenden Benennung eines betrieblichen Datenschutzbeauftragten auf 20 Personen noch nicht nachvollzogen. Ob dies im Rahmen der derzeit laufenden Evaluierung des kirchlichen Gesetzes angedacht wird, ist noch nicht bekannt.

14 Die 27 (Erz-)Diözesen haben fünf gemeinsame Datenschutzaufsichten bestellt mit Sitzen in Bremen, Schönebeck, Dortmund, Frankfurt am Main und München. Daneben gibt es eine gemeinsame Datenschutzaufsicht für die Ordensgemeinschaften päpstlichen Rechts in Deutschland. Die EKD hat mit dem Beauftragten für den Datenschutz mit dem Hauptsitz in Hannover und vier Außenstellen eine Datenschutzaufsicht eingerichtet, der sich die überwiegende Mehrzahl der Landeskirchen und Diakonischen Werke angeschlossen haben.

15 Die Beschlüsse sind über die Internetseiten der kirchlichen Datenschutzaufsichten abrufbar, z.B. unter www.katholisches-datenschutzzentrum.de in der Rubrik Infothek.

16 Während § 47 DSG-EKD zumindest teilweise noch ein Vorverfahren fordert, verzichtet das KDG auf die Durchführung eines Vorverfahrens.

17 Unter der Adresse https://www.dbk.de/themen/kirche-staat-und-recht/kirchliche-gerichte-in-datenschutzangelegenheiten/ sind weitere Informationen zu beiden Instanzen abrufbar, u.a. auch die Entscheidungen. Eine erste Betrachtung der Arbeit des Gerichtes enthält Sydow, Die Datenschutzgerichte der katholischen Kirche – erste Erfahrungen und Perspektiven, in: Pau (Hrsg.), Ein Jahr Gesetz über den Kirchlichen Datenschutz (KDG) – Rückblick und Ausblick, Katholisches Datenschutzzentrum, Dortmund 2020, S. 53 ff. (online abrufbar). Eine Übersicht über die ersten veröffentlichten Entscheidungen enthält der Beitrag von Joachimski/Melzow, Die kirchliche Datenschutzgerichtsbarkeit, in: Pau (Hrsg.), Kirchlicher Datenschutz – gewachsener Baustein kirchlicher Selbstverwaltung, Katholisches Datenschutzzentrum, Dortmund 2021, S. 91 ff. (online abrufbar).



St. Nepomuk – Schutzheiliger des Beichtgeheimnisses. Bild: Wikipedia – gemeinfrei.



St. Ivo Hélory von Kermatin – Schutzpatron der Datenschützer. Bild: Wikipedia – gemeinfrei

Heinz Alenfelder

Die Entwicklung einer Smart City – Im Fokus: Bürgerbeteiligung

Nach aktuellen Vorhersagen[1] werden in der Mitte dieses Jahrhunderts über zwei Drittel der Menschheit in Städten leben. Die damit einhergehenden Herausforderungen sollen – vor allem nach Vorstellungen der großen Technologiekonzerne – mit dem Konzept der Smart City gelöst werden. Meist laufen diese Vorstellungen auf eine Totalvernetzung im sogenannten Internet of Things hinaus: Sensoren, Kleinstcomputer und Mobilgeräte liefern Unmengen von Daten, die in der Cloud ausgewertet und zur „smarten" Steuerung des gesamten städtischen Lebens verwendet werden können. Anlässlich der Verleihung des BigBrotherAwards in der Kategorie PR und Marketing an das Konzept Smart City formulierte die Laudatorin Rena Tangens 2018: „Eine Smart City ist die perfekte Verbindung des totalitären Überwachungsstaates aus George Orwells 1984 und den normierten, nur scheinbar freien Konsumenten in Aldous Huxleys Schöne Neue Welt"[2]. In diesem Beitrag werden einige Ratgeber zur Entwicklung einer Stadt zur Smart City unter dem Blickwinkel der demokratischen Beteiligungsrechte und der Beachtung der Grundrechte betrachtet. Auf die spezielle Datenschutzproblematik geht Astrid Donaubauer-Grobner in dem folgenden Artikel ein.

Das Bundesministerium für Wohnen, Stadtentwicklung und Bauwesen hat mit www.smart-city-dialog.de eine Plattform geschaffen, die helfen soll „Smart Cities gemeinsam im Dialog zwischen Politik, Verwaltung, Wirtschaft, Wissenschaft und Zivilgesellschaft zu gestalten". Konkret zuständig ist das Bundesinstitut für Bau-, Stadt- und Raumforschung (BBSR) im Bundesamt für Bauwesen und Raumordnung (BBR). Seit 2016 werden in dem Dialog-Projekt Leitlinien und Handlungsempfehlungen entwickelt, die zur Smart City Charta[3] führten, mit der es Kommunen ermöglicht werden soll „die Digitalisierung aktiv und zielgerichtet zu gestalten."

Um die Ziele der Charta zu konkretisieren haben Tristan Fuhrmann, Paul Böttcher und Kathrin Bimesdörfer von der ifok GmbH im Herbst 2021 „Datenstrategien für die gemeinwohlorientierte Stadtentwicklung"[4] beschrieben. Neben Kompetenzzentren empfehlen sie Digitallotsen und „Datenbeiräte mit Mitgliedern aus der Zivilgesellschaft". Anhand von „gemeinsam festgelegten Grundwerten und Prinzipien" sollen beim Umgang mit personenbezogenen Daten auch Datenschutz und informationelle Selbstbestimmung sichergestellt werden. Interessant an den Empfehlungen ist, dass die zu entwickelnden Prinzipien „über die notwendige Kenntnis und Einhaltung bestehender gesetzlicher Vorgaben hinausgehen" und vor allem die Bereiche berücksichtigen sollen, die noch nicht reglementiert sind. Zu den Themen „Datenethik", „Datenschutz und informationelle Selbstbestimmung" sowie „Datensicherheit" und „Datenverantwortung" werden konkrete Handlungsempfehlungen gegeben. Ein Beispiel: „Städte und Landkreise sollten als Datenschutz-Vorreiter auch neue Konzepte zur Stärkung des Grundrechts auf informationelle Selbstbestimmung erproben." Oder auch die folgende Aussage, der uneingeschränkt zuzustimmen ist: „Durch die Nutzung datenbasierter Anwendungen in der Smart City dürfen keine Gefahren für die Grundrechte, die Sicherheit, die Freiheitsrechte und die Privatsphäre der Menschen entstehen."

Aus weiteren Modellprojekten des BBSR werden dann auch Anregungen entwickelt, die sich auf die Bürgerbeteiligung konzentrieren. So in einem Erfahrungsbericht[5], in dem beispielsweise bezogen auf Wilhelmshaven das Fazit gezogen wird: „Neben der Beteiligung von Expertinnen und Experten wird die Beteiligung von Bürgerinnen und Bürgern sowie gesellschaftlichen und sozialen Einrichtungen als wichtige Grundlage für die Entwicklung von bedarfsorientierten Lösungen vor Ort angesehen." Wie eine solche Einbindung funktionieren kann, untersuchte bereits 2017, d.h. vor dem Schub, den die Corona-Pandemie der Digitalisierung verpasste, eine Studie zum Einsatz webbasierter Medien in der Stadtentwicklung[6] und kam dabei zu sieben Erkenntnissen:

- Die untersuchten Akteure und Akteurinnen setzen neben Online-Formaten auch Bürgerversammlungen ein, um eine größere Beteiligung zu erreichen.
- Stadtverwaltungen tun sich schwerer beim Einsatz Sozialer Medien als zivilgesellschaftliche Gruppen.
- Die Möglichkeiten des Einsatzes webbasierter Medien sind für öffentliche Stellen durch stärkere Regulierungen eingeschränkt.
- Neue „intermediäre Akteure" nehmen selbst erheblichen Einfluss auf die Ausgestaltung der Partizipation.
- Das Vertrauen in die Verwaltung kann durch die mit webbasierten Medien geschaffene Transparenz gestärkt und die Akzeptanz von Entscheidungen erhöht werden.
- Der Einsatz webbasierter Medien in der Stadtentwicklung erfordert weitere Ressourcen.
- Die Effizienz von Verfahren der Verwaltung kann durch den Einsatz webbasierter Medien gesteigert werden.

Allerdings werden am Schluss die „Unsichtbaren", also Menschen mit geringerem Bildungsstand und Einkommen, weiterhin nicht erreicht und können sich nicht einbringen. Insofern etabliert sich auch hier eine Situation, wie sie von Kurt Vonnegut schon 1952 in seinem Roman „Player Piano" hervorragend und zukunftsweisend beschrieben wurde: Eine „Kaste" von Ingenieuren mit hohem Intelligenzquo-

tient betreut lediglich Maschinen, die die Produktion anpassen auf den von ihnen selbst errechneten Bedarf der mittlerweile weitgehend arbeitslosen Bevölkerung Amerikas. Die Mitglieder dieser Kaste wohnen auch räumlich abgetrennt von der wohlhabenden Elite. Was damals als „Science Fiction" vermarktet wurde, ist heute in der Neoliberalität moderner Stadtentwicklung wiederzufinden.

Der Deutsche Städtetag („Die Stimme der Städte") berät seine Mitglieder mit einer Publikation[7] dabei, wie sie die „Stadt der Zukunft" mit Daten gestalten sollen. Im Vordergrund steht die Datensouveränität beim Ausbau der Infrastruktur und die Frage, wie Städte sicherstellen, dass sie „die Daten entsprechend ihrem Selbstverständnis nutzen können". Wenn auch die Rechte der Bürgerinnen und Bürger eher am Rande betrachtet werden, so liefert die Handreichung doch eine recht umfassende Übersicht über die verschiedenen gesetzlichen Grundlagen, angefangen von der PSI-Richtlinie ((EU) 2019/1024) über das Informationsweiterverwendungsgesetz (IWG) sowie das Informationsfreiheitsgesetz (IFG) des Bundes bis zur Länderebene. Sie bietet darüber hinaus Musterregelungen verschiedener Städte an, wie beispielsweise die Datennutzungsklauseln von Bonn und Münster oder per Verweis das Datenethik-Konzept der Stadt Ulm[8]. Vielfältig ist außerdem die Vorstellung von Anwendungsfällen, die vom Energie-Monitoring (Cottbus) über eine integrierte Sozialplanung (Emden) bis zum zentralen Geodaten-Management (Nürnberg) reichen.

Eine ebenfalls große Übersicht über Anwendungen in 14 Smart Cities haben Meiyi Ma und andere bereits 2019 publiziert[9]. Auch aus dem Jahr 2019 stammt der Smart-City-Atlas[10] des IT-Branchenverbands Bitkom, in dem „eine strukturierte Übersicht der 50 Vorreiterstädte in Deutschland" gegeben wird. Als Schwerpunkte der Bürgerbeteiligung nennt das Autorenteam: Vernetzung von Akteuren sowie die Informationsvermittlung und Sammlung von Ideen. Allerdings wird auch konstatiert, dass „die meisten Städte noch zurückhaltend sind, was den Einsatz digitaler Möglichkeiten zur Bürgerbeteiligung angeht". Dabei hat ein Team der Universität Kassel um Matthias Simon Billert im Rahmen des Forschungsprojekts Civitas Digitalis ausführliche Handlungsempfehlungen[11] für die Erstellung von bürgerinitiierten Dienstleistungen formuliert, die zuallererst fordern: „Einbindung von Bürgerinnen und Bürgern als Prosumenten: Sie produzieren ihre eigenen Dienstleistungen, die sie im Anschluss selbst konsumieren".

Schließlich entwarf Eduard Itrich im Auftrag des Fritz-Erler-Forums Baden-Württemberg (Friedrich-Ebert-Stiftung) einen Ratgeber für Kommunen, damit diese die Digitalisierung souverän gestalten[12]. Der deutlich technisch ausgerichtete Leitfaden fordert unter der Überschrift „Open Community – gemeinsam statt einsam" aber auch eine enge Zusammenarbeit eines kommunalen Digitalisierungs-Beauftragten mit der Zivilgesellschaft, der Wirtschaft und benachbarten Kommunen sowie niedrigschwellige Beteiligungsmöglichkeiten. Nötig dafür sei „eine offene Infrastruktur für bestmögliche Partizipationsmöglichkeiten", denn die Kommune gehöre „zu den wichtigsten Treibern einer gemeinwohlorientierten Gestaltung der Digitalisierung". Den Gedanken der Partizipation unterstützte auch Volker Kefer vom VDI 2019 beim Vorstellen einer Studie zum automatisierten Fahren in der Smart City[13]: „Wir brauchen Öffentlichkeitsarbeit, Bürgerdialoge und Beteiligungsmöglichkeiten, bei denen Bürgerinnen und Bürger aktiv bei der Ausgestaltung der Mobilität in der Smart City eingebunden werden […] nur so können wir sicherstellen, dass die Potenziale des technischen Fortschritts auch allen zugutekommen."

In Bezug auf den Datenschutz bleibt zu hoffen, dass die Arbeit des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Ulrich Kelber, fruchtet. Er schreibt in seinem 30. Tätigkeitsbericht für 2021[14], dass er sich als Vorsitzender der „Internationalen Arbeitsgruppe zum Datenschutz in der Technologie" für eine weiterhin hohe Qualität der Ergebnisse auch zum Thema „intelligente Stadt (‚Smart Cities') sowie Gesichtserkennungstechnologie" einsetzen werde.

1 https://www.zukunftsinstitut.de/artikel/urbanisierung-die-stadt-von-morgen

2 DANA 2/2018, S. 95

3 https://www.smart-city-dialog.de/wp-content/uploads/2021/04/2021_Smart-City-Charta.pdf

4 https://www.smart-city-dialog.de/wp-content/uploads/2021/12/datenstrategien-gemeinwohl-stadtentwicklung-dl.pdf

5 https://www.bbsr.bund.de/BBSR/DE/veroeffentlichungen/exwost/52/exwost-52-2-dl.pdf

6 https://www.bbsr.bund.de/BBSR/DE/veroeffentlichungen/bbsr-online/2017/bbsr-online-28-2017-dl.pdf

7 https://www.staedtetag.de/files/dst/docs/Publikationen/Weitere-Publikationen/2021/stadt-der-Zukunft-mit-daten-gestalten-studie-2021.pdf

8 https://www.zukunftsstadt-ulm.de/sites/default/files/downloads/ulm-201008-txt-datenethikkonzept-stadt-ulm-final.pdf

9 https://dl.acm.org/doi/10.1145/3355283

10 https://www.bitkom.org/sites/default/files/2019-03/190318-Smart-City-Atlas.pdf

11 https://civitas-digitalis.informatik.uni-hamburg.de/wp-content/uploads/2019/11/Handlungsbroschüre-zum-Verbundforschungsprojekt-Civitas-Digitalis.pdf

12 https://library.fes.de/pdf-files/bueros/stuttgart/19112.pdf

13 https://www.vdi.de/news/detail/vdi-studie-bevoelkerung-unterschaetzt-potenziale-des-automatisierten-fahrens

14 https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/30TB_21.pdf, Seite 28


Bild: iStock.com/greenbutterfly

Astrid Donaubauer-Grobner

Smart Cities und Datenschutz (in Österreich)[1]


Bild: iStock.com/chombosan

Smart liegt im Trend – ob es sich um Haushaltsgeräte, Wearables, Transportmittel und natürlich Mobiltelefone handelt. Diese Entwicklung verspricht – und hält – mehr Bequemlichkeit für die Endnutzer*innen durch automatische Koordination von Abläufen im Hintergrund und ermöglicht neue Handlungsspielräume. Dass im Hintergrund Daten über das Nutzer*innenverhalten gesammelt, verwertet und oft auch zur Erstellung von Profilen verwendet werden, ist einem Teil der, aber keineswegs der gesamten Zielgruppe bewusst. Oftmals zeigt das Argument „man hätte nichts zu verbergen" fehlendes Wissen über den Umstand, dass Verhaltensdaten Individuen anfälliger für Manipulation werden lassen (Solove, 2007). In der Privatwirtschaft dient dies mehrheitlich dem Zweck der Kaufanimation durch zielgerichtete individualisierte Werbemaßnahmen, die eine stärkere Wirkung zeigen und weniger Kosten mit sich bringen als generalisierte Massenwerbung (Zuboff, 2019). Daten besitzen einen beträchtlichen ökonomischen Wert. Die Forbes-Liste (Forbes, 2020) zeigt, dass Technologie-Giganten wie Apple, Google, Microsoft, Amazon und Facebook, deren Produkte und Dienstleistungen große Mengen an Nutzer*innendaten generieren, die einst mächtigen Ölkonzerne von der Spitze der umsatzstärksten Unternehmen vertrieben haben. Daten sind mittlerweile ein Rohstoff, das daraus gewonnene Produkt ist die Verhaltensmodifikation der Nutzer*innen (Zuboff, 2019).

Dieser Trend erstreckt sich allerdings über privatwirtschaftliche Aktivitäten hinweg auch auf Staaten. Denn basierend auf vergangenheitsbezogenen individuellen, digitalen Daten lassen sich Vorhersagen machen und diese können auch für die Modifikation von zukünftigem Verhalten herangezogen werden (Zuboff, 2019). Smart Cities sind die Kerbe, in die Länder in unterschiedlichem Ausmaß je nach rechtlicher Lage und finanziellen Möglichkeiten schlagen. Auch hier ist das Sammeln von Daten und deren Verarbeitung ein kritisches Thema, das die Grundrechte der Bürger*innen und in der Folge die Aufrechterhaltung demokratischer Prinzipien betrifft. Dies bezieht sich speziell auf die bereits erwähnten Möglichkeiten zu Verhaltensmanipulationen, die mit Blick auf das internationale politische Parkett speziell mit zwei prominenten Beispielen in Verbindung gebracht werden: der Wahl von Donald Trump in den USA und dem Brexit (Ausstieg des UK aus der EU).

Dies war speziell durch die gezielte Nutzung von sozialen Medien möglich. Hier lässt sich nun die Brücke zu Smart City-Konzepten schlagen: Kommen zu diesen in der Regel freiwillig bereitgestellten Daten dann noch Informationen von Bürger*innen hinzu, die deren tägliches Umfeld, Bewegungsprofile, Urlaubsgewohnheiten, Stromverbrauchsgewohnheiten etc. beinhalten, lassen sich detaillierte Profile erstellen, die dem Staat intimere Kenntnisse über die Einzelperson erlauben als jedem Familienmitglied im gleichen Haushalt. Die Konsequenz daraus ist eine gewisse Angreifbarkeit der Bürger*innen gegenüber staatlichen Organen. Die Integrität eines politischen Apparates ist eine Momentaufnahme der zu jedem Zeitpunkt im Amt befindlichen Akteur*innen – und deren persönlicher Integrität.

Dieser letzte Punkt sei speziell im Zusammenhang mit Österreich erwähnt, dessen politische Landschaft in den vergangenen Jahren (beziehungsweise bereits Jahrzehnten) von Korruptionsskandalen erschüttert wurde. Erst 2021 führte die Enthüllung von gekauften Umfragen zur öffentlichen Meinung mit dem Ziel der Bürger*innenbeeinflussung zum Ende der Ära Kurz als Kanzler. Zuvor führte die Aufdeckung des sogenannten Ibiza-Skandals, der unter anderem den Aspekt der geplanten Steuerung der auflagenstärksten Zeitung Österreichs zugunsten der involvierten politischen Akteure enthielt, 2019 zum Auseinanderbrechen der amtierenden Regierung des Landes. Wegen des Beispiels Österreichs, eines Industrielandes in Mitteleuropa, eines Mitglieds der EU, wo Manipulation der öffentlichen Meinung durchaus nachweislich in höchsten politischen Kreisen betrieben wurde, ist es also durchaus eine berechtigte Frage, welche Daten einem Staat sinnvoll anvertraut werden sollten.

Im Fall von Smart Cities allerdings ist Bequemlichkeit nicht das einzige Argument, das für solch ein Konzept spricht. Speziell im Angesicht der Klimakrise wären Daten über Konsumverhalten, Verbrauchs- und Heizgewohnheiten, Mobilität und so weiter wertvolle Ansatzpunkte, um Problemlösungsstrategien für die Herausforderungen in Ballungsräumen zu erarbeiten, die sich an der Realität orientieren anstatt auf vagen Annahmen zu basieren. Daraus ergibt sich also ein Spannungsfeld von Chancen und Bedrohungen.

Zur Bewältigung dessen braucht es verbindliche Rahmenbedingungen, die die Erschaffung von Smart-City-Strukturen ermöglichen ohne damit die Prinzipien der Demokratie durch exzessive Überwachung und Missbrauch von gesammelten Bürger*innen-Daten zu gefährden.

In Österreich ist im Jahr 2021 die gesetzliche Lage zum Datenschutz durch die unmittelbar anwendbare Datenschutz-Grundverordnung 2016/679 (DSGVO) geprägt – und zusätzlich von den zahlreichen gesonderten Gesetzen, die nicht von der DSGVO direkt geregelt sind, wie z.B. Arbeitsverfassungsgesetz, Bundesabgabenordnung, E-Commerce-Gesetz, Gewerbeordnung, Meldegesetz, Sicherheitspolizeigesetz, Verbraucherkreditgesetz.

Was die Umsetzung der DSGVO in Österreich betrifft, ist das Land jedoch mit Kritik konfrontiert. Diese richtet sich speziell daran, dass Öffnungsklauseln in der DSGVO, die den einzelnen Staaten in gewissen Bereichen Regelungen nach eigenem Ermessen ermöglichen, zur Abschwächung der Datenschutz-Grundverordnung genutzt wurden – mit dem wenig subtil benannten Datenschutz-Deregulierungsgesetz 2018, dem Datenschutzänderungsgesetz 2018 und dem novellierten Datenschutzgesetz. Darin wurde festgelegt, dass Unternehmen bei Erstverstößen keine empfindlichen Geldbußen auferlegt werden sollen, sondern lediglich Verwarnungen. Und auch, dass öffentliche Stellen sowie privatrechtlich agierende Stellen mit gesetzlichem Auftrag von der DSGVO ausgenommen werden sollen und damit bei Verstößen straffrei ausgehen. Datenriesen wie Facebook und Google mit Sitz außerhalb von Österreich können nur unter erschwerten Bedingungen von Verbänden verklagt werden. Für journalistische, wissenschaftliche, künstlerische oder literarische Zwecke wird der Datenschutz aufgeweicht. Hinsichtlich smarter urbaner Lebensräume gibt es noch zwei relevante Bestimmungen aus dem Datenschutz-Deregulierungsgesetz 2018: Betroffene Personen können von Akteuren im staatlichen Auftrag keine Auskünfte erhalten, wenn dies die Erfüllung der übertragenen Aufgabe gefährdet. Und Bildaufnahmen sind auch dann zulässig, wenn ein gelinderes Mittel ebenso geeignet wäre und zur Verfügung stünde.

In der Abstimmung zur EU-DSGVO 2015 stimmten nur 2 von 28 Ländern dagegen – Österreich und Slowenien. Der Argumentation aus Österreich, man wäre wegen einer Aufweichung des hohen Datenschutzniveaus durch EU-Bestimmungen besorgt, widersprechen die in der Folge erlassenen Gesetze zur Auflockerung der EU-Verordnung deutlich. Damit liegt nahe, dass die rechtliche Situation zum Datenschutz in Österreich, die verstärkt auf die Bedürfnisse datengetriebener privatwirtschaftlicher Unternehmen und damit weniger auf die Schutzbedürfnisse der Bürger*innen abgestimmt ist, kaum als idealer Rahmen für demokratisch ausgestaltete Smart-City-Konzepte betrachtet werden kann.

Dieser kurze Umriss zeigt ein wenig wünschenswertes Vorgehen von staatlicher Seite. Wie aber könnte ein konstruktiver, demokratiekonformer Umgang mit Daten und Bürger*innenrechten aussehen? Dazu gibt es aus den USA ein best-practice-Beispiel. In Zanesville, Ohio, werden in Form von Open-Government-Data-Initiativen Daten der Öffentlichkeit zugänglich gemacht und können als Basis für Diskurse über demokratische Interessen herangezogen werden. Somit sind die Daten allen betroffenen und interessierten Seiten gleichermaßen zugänglich – und können von diesen auch entsprechend interpretiert werden ohne der Deutungshoheit durch den Staat zu unterliegen (Mämecke et al., 2017). Die Offenlegung von Daten, sofern weder Datenschutz noch Sicherheit dadurch gefährdet werden, ermöglicht die Partizipation der Stadtbewohner*innen und erhöht die Bürger*innennähe (Walser & Haller, 2016). Ein weiterer Aspekt im Umgang mit Daten ist die Frage, wer sie sammelt, speichert, auswertet und verteilt. Social-Media-Plattformen beispielsweise sind kaum vereinbar mit Datenschutz (Datenschutz.org, 2020) und bekämpfen Auflagen zum Datenschutz, womit sie zum Nachteil der Nutzer*innen agieren (Constine, 2018; Scola, 2018). Da allerdings genau diese Daten für staatliche Zwecke ebenfalls von Interesse sind, stärkt das die Position dieser Plattformbetreiber und schwächt somit jene der Bürger*innen. Daraus ergibt sich, dass sich Datenquellen, Infrastrukturen und Services für Smart City-Initiativen (z.B. Telekommunikation, Energieversorgung, Cloud-Speicherdienste) entweder in öffentlichem Besitz, zumindest aber unter öffentlicher Kontrolle befinden sollten, damit den Rechten von Bürger*innen Vorrang vor privatwirtschaftlichen Interessen eingeräumt wird (Walser & Haller, 2016).

Weshalb genau ist das Sammeln, Interpretieren und Verteilen gewisser personenbezogener Daten solch ein beträchtliches potentielles Risiko für Bürger*innen? Zusätzlich zu dem zuvor bereits angesprochenen Aspekt der Manipulierbarkeit von Handlungen im Sinne von konsumbezogenen wie auch politischen Entscheidungen kommt die Tatsache hinzu, dass Aufzeichnungen über Handlungen diese Handlungen überdauern – und auch außerhalb des Internets Konsequenzen haben können. Erhalten Banken, Versicherungen oder mögliche Arbeitgeber Zugriff auf diese Daten, kann dies das Zustandekommen einer Geschäftsbeziehung mit der Institution maßgeblich beeinflussen (Löw & Rothmann, 2016). Deshalb braucht es vertrauenswürdige Einrichtungen zum Schutz der Persönlichkeitsrechte, die ständig kontrollieren, ob die Systeme noch verlässlich sind und die Verlässlichkeit gegebenenfalls wiederherstellen können (Löw & Rothmann, 2016).

Als Gegenpol zu Zanesville, Ohio, im Umgang mit personenbezogenen Daten bietet sich das Social-Credit-System (SCS) in China an. Dort wird durch eine zentrale Dateninfrastruktur Datensammlung, Data Mining und Analyse betrieben (Diab, 2017). Darauf aufbauend wird dann das soziale Verhalten in

den vier Bereichen Regierungsangelegenheiten, Rechtliches, Soziale Aktivitäten und Verbraucherverhalten bewertet und als Basis für Belohnung oder Bestrafung herangezogen (Liang et al., 2018). Zugang zum Wirtschafts- und Finanzsektor erhält nur, wer sich den Regeln der herrschenden Partei beugt (Meissner & Wübbeke, 2016). In China kooperieren seit 2010 rund 500 Städte mit IT-Unternehmen im Hinblick auf die Sektoren Transport, Verwaltung und Gesundheitssystem – und Überwachung durch mehr als 20 Millionen Straßenkameras, mit denen nicht nur kriminelle Aktivitäten dokumentiert, sondern Individuen mittels Gesichtserkennung verfolgt werden (Liang et al., 2018). Überwachungsmechanismen sind im Zeitalter von Big Data nicht mehr länger offensichtlich im Sinne einer gut sichtbaren Kamera (Tufekci, 2014), sondern sind speziell in China unsichtbar und mit Algorithmen ausgestattet, die auf die politischen Ziele der Regierung ausgerichtet sind (Meissner & Wübbeke, 2016). An diesem Beispiel zeigt sich, dass der private Sektor beim Aufbau weitreichender Überwachungssysteme unvermeidbar ist. In der Harvard Law Review (2018) werden Datenkonzerne wie Facebook, Twitter und Google als Überwachungs-Vermittler (surveillance intermediaries) bezeichnet.

Wie lässt sich diesen düsteren Aussichten auf totale Überwachung durch private und staatliche Akteure ohne jeden Fokus auf Bürger*innenrechte oder demokratische Prinzipien also begegnen? Eine Option wäre der Verzicht auf Smart-City-Initiativen, der jedoch auch mit dem Verzicht auf bessere Lebensqualität, verstärkte Resilienz (speziell in Krisenzeiten) und gesteigerte Nachhaltigkeit (Donaubauer-Grobner, 2021) einhergehen würden, da zielgerichtete Erfassung und Verwertung von Daten zu raschen und effektiven Lösungen führen kann. Helbing (2019) spricht sich für folgende Maßnahmen aus, um den Gefahren der Grundrechtsverletzung durch datengetriebene Technologie zu begegnen:

- Demokratische Kontrolle der Instrumente durch das Parlament anstatt durch Kanzler/Präsident, Militär, Regierungsparteien oder Geheimdienste
- Zugriff auf diese Systeme auch für Oppositionsparteien zur Pflege pluralistischer Perspektiven
- Einsatz dieser Instrumente mit demokratischem Mandat und auf Basis wissenschaftlicher Prinzipien
- Sicherstellung ethischer Überwachung
- Anonymisierung persönlicher Daten und Ahndung von Verletzungen der Privatsphäre
- Transparenz über Aufzeichnungen, wer das System in welcher Weise nutzt, mit regelmäßigen, verständlichen Berichten an die Öffentlichkeit
- Möglichkeiten des Opt-out (= Entscheidung nicht teilzunehmen) zur Sicherstellung von Informations-Selbstbestimmung
- Angemessene Entschädigung von Opfern bei unerwünschten Nebenwirkungen sozialer Experimente
- Verbot von großangelegtem Nudging (= mehr oder weniger subtiles Anregen von Handlungen/Verhaltensweisen; Bendel, 2019)
- Verbot von Massenüberwachung, Aufhebung der Anonymisierung nur für kleine Personengruppen und unter demokratischer Kontrolle
- Fokus auf Sicherheitsaspekte mittels Schutz vor unbefugtem Zugriff auf Daten durch bessere Verschlüsselung
- Dezentrale Lagerung von Daten, sodass kein Zugriff auf große Datenmengen mit einem einzigen Passwort erfolgen kann

Manche dieser vorgeschlagenen Maßnahmen spiegeln sich auch in den Wünschen von Städteplaner*innen in österreichischen Landeshauptstädten wider, die folgende Voraussetzungen für eine datenschutz- und demokratiekonforme sowie resilienzsteigernde Umsetzung von Smart-City-Projekten für erforderlich halten (Donaubauer-Grobner, 2021):

1) Informed Consent (informierte Zustimmung)

Bürger*innen müssen vor Beginn eines Smart-City-Projekts mit jenen Informationen versorgt werden, die ihnen eine informierte Entscheidung und Teilhabe ermöglichen. Dazu gehört auch die Kommunikation von möglichen Nachteilen, die in der Praxis jedoch meist unterbleibt.

2) Opt-out-Möglichkeiten (Verweigerung der Zustimmung zur Erhebung der Daten)

Bürger*innen müssen – besonders im Fall von versorgenden Infrastrukturleistungen wie öffentlicher Mobilität, Elektrizität etc. – die Möglichkeit haben die Preisgabe ihrer Daten zu verweigern ohne dadurch von der Leistung ausgeschlossen zu werden.

3) Data Ownership (Eigentum an den erhobenen Daten)

Smart Cities generieren große Mengen an Daten, die einen klaren ökonomischen Gegenwert haben und damit Interessenten aus dem freien Markt anlocken. Während die öffentliche Verwaltung im Hinblick auf internationale Beispiele für Überwachungsstaaten als Gegenpol zu Bürger*inneninteressen betrachtet werden kann, so ist dies im Fall von privatwirtschaftlichen Akteuren als Eigentümer*innen der personenbezogenen Bürger*innendaten, die im Zuge einer hoheitlichen Stadtentwicklungsmaßnahme erhoben wurden, eine noch beträchtlichere Gefahr für die Rechte der Stadtbewohner*innen.

4) Umsetzung des Datenschutzes

Die DSGVO wurde auf nationaler Ebene um weitere Gesetze ergänzt, die im Vergleich mit anderen EU-Staaten zu einer vergleichsweise unternehmer*innenfreundlichen Rechtslage hinsichtlich des Datenschutzes beitragen. Beispielsweise wurde nach Ende der Übergangsfrist mit dem verbindlichen Inkrafttreten der DSGVO in Österreich beschlossen, es möge primär Verwarnungen anstatt der Verhängung der beträchtlichen Geldstrafen bei Verstößen gegen die Datenschutzbestimmungen geben. Gleichzeitig wurde vom Gesetzgeber jedoch unterlassen Richtlinien und Orientierungsgesetze für öffentliche Verwaltungen bereitzustellen, um ihnen einen datenschutz- und demokratiekonformen Umgang mit den personenbezogenen Daten ihrer Bürger*innen zu erleichtern.

5) Datenminimierung und Zweckbindung

Dabei handelt es sich um zwei der Grundsätze des Artikel 5 (1) DSGVO, die sicherstellen sollen, dass Daten nicht entsprechend technischer Möglichkeiten in großem Stil, sondern abhängig von dem dahinterliegenden Zweck gesammelt werden. Während für Städte mit großangelegten Datensammelinitiativen auch erhöhte Infrastrukturkosten

für die Verarbeitung und Speicherung dieser Daten einhergehen, ist diese Vorgehensweise für private Akteure weniger problematisch, da Daten auf dem freien Markt einen gewinnbringenden Gegenwert haben – weshalb Datenminimierung und Zweckbindung nicht in ihrem Interesse liegen und damit einen Konflikt mit Bürger*inneninteressen darstellen.

6) Anonymisierung, Pseudonymisierung und Aggregierung

Ist für die Zwecke einer Smart-City-Initiative die Erfassung personenbezogener Daten erforderlich, so sollten geeignete Maßnahmen getroffen werden, um den Personenbezug nicht länger als erforderlich zu erhalten. Im Idealfall erfolgt die Maßnahme bereits unmittelbar nach der Erfassung, sodass Erfassungsinstrumente bereits anonymisierte oder aggregierte Daten weiterleiten, bevor diese gespeichert werden.

7) Politische Rahmenbedingungen

Eine maßgebliche Rahmenbedingung ist die Vergabe von Fördergeldern durch die öffentliche Hand, da private Finanzierungsmöglichkeiten in der Regel auch mit mehr Mitbestimmungsrecht, unter anderem über das Eigentum und die Verwendung der erhobenen personenbezogenen Daten, einhergehen. Eine Veränderung der politischen Landschaft der Stadt-, Landes- oder Bundesregierung zugunsten anderer Fraktionen kann für ein laufendes Projekt ebenfalls ein Versiegen der finanziellen Mittel zur Folge haben. Auch die unter 4) angeführte Umsetzung des Datenschutzes, die angesprochenen erforderlichen rechtlichen Orientierungshilfen sowie das Commitment zur Miteinbeziehung der Bürger*innen in Smart-City-Initiativen fallen unter die politischen Rahmenbedingungen.

Die aktuelle Lage in Österreich im Bereich der Städteplanung bei Smart-City-Initiativen ist eine heterogene – allerdings nicht primär im positiven Sinn von bestehenden Möglichkeiten zur Entfaltung und kreativer Ergebnisoffenheit, sondern hinsichtlich fehlender Rahmenbedingungen, die eine Orientierung ermöglichen. Das betrifft speziell das Verständnis zum Umgang mit personenbezogenen Daten und den Möglichkeiten dahinter (z.B. Profiling), die in unterschiedlichen Landeshauptstädten gelebt werden. Es gibt Verfechter beider Enden des Spektrums und natürlich mehrere Nuancen dazwischen: Einerseits „Es ist alles erlaubt, was nicht explizit laut Gesetz verboten ist" – mit allem, was sich daraus in einem Land mit einem klaren Commitment zu wenig Auflagen für den Datenschutz ableiten lässt. Und auf der anderen Seite an anderen Standorten die Scheu davor Projekte in Angriff zu nehmen, weil keine explizite Rechtssicherheit für die hoheitliche Verwendung der gesammelten Daten besteht und die Verletzung von Rechten der Bevölkerung als zu großes Risiko erachtet wird. Ebenso bestehen bei zuständigen Stellen für Smart-City-Projekte unterschiedliche Ansichten darüber, ob es einer verstärkten Regulierung durch gesetzliche Vorgaben bedarf, die eben Rechtssicherheit schaffen aber auch zwangsläufig gewisse Freiheiten eindämmen würde. Derzeit basiert die Einschätzung der rechtlichen Lage und die daraus resultierende Städteplanung auf der Interpretation von Einzelpersonen anstatt auf universell gültigen Rahmenbedingungen zum Schutz personenbezogener Daten und damit ziviler Rechte. Das mag in Zukunft zu neuen Ausprägungen von Korruption oder fehlender Städteentwicklung der Bürger führen und damit auch zur Wahrnehmung von Lebensqualität in einzelnen Städten beitragen.

Literatur:

Constine, J. (2018). A flaw-by-flaw guide to Facebook's new GDPR privacy changes. https://techcrunch.com/2018/04/17/facebook-gdpr-changes/

Datenschutz.org. (2020). Datenschutz in sozialen Netzwerken: Sehen und gesehen werden. VFR Verlag für Rechtsjournalismus. https://www.datenschutz.org/soziale-netzwerke/

Diab, R. S. (2017). Becoming-Infrastructure: Datafication, Deactivation and the Social Credit System. Journal of Critical Library and Information Studies, 1(1), 1–23. 10.24242/jclis.v1i1.19

Donaubauer-Grobner, A. (2021). Smart Cities und Demokratie – Ein Widerspruch? Publikationsdatenbank FH Campus Wien

Forbes. (2020). The world's most valuable brands. https://www.forbes.com/the-worlds-most-valuable-brands/

Helbing, D. (2019). Towards Digital Enlightenment: Essays on the Dark and Light Sides of the Digital Revolution. Springer

Liang, F., Das, V., Kostyuk, N. & Hussain, M. M. (2018). Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure. Policy & Internet, 10(4), 415–453.

Löw, M. & Rothmann, L. (Hg.). (2016). Privatsphäre in Smartcities. Eine raumsoziologische Analyse. In: Smart City. Strategie, Governance und Projekte. Springer Vieweg.

Mämecke, T., Passoth, J.-H. & Wehner, J. (Hg.). (2017). Bedeutende Daten. Modelle, Verfahren und Praxis der Vermessung und Verdatung im Netz: Pleasing Little Sister. Big Data und Social Media Surveillance. Springer.

Meissner, M. & Wübbeke, J. (2016). IT-backed authoriatrianism: Information technology enhances central authority and control capacity under Xi Jinping(1), 52–57.

Scola, N. (2018). Facebook enlists conservative help to resist privacy rules: An email seeking U.S. groups' assistance against EU-style regulations came as Mark Zuckerberg was preparing to testify to Congress. Politico. https://www.politico.com/story/2018/04/17/facebook-conservatives-privacy-rules-489242

Solove, D. J. (2007). I've Got Nothing to Hide and Other Misunderstandings of Privacy. San Diego Law Review(44), 745–772.

Tufekci, Z. (2014). Engineering the Public: Big Data, Surveillance and Computational Politics. First Monday, 19(7), 1–16. 10.5210/FM.V19I7.4901

Walser, K. & Haller, S. (Hg.). (2016). Smart Governance in Smart Cities. In: Smart City. Strategie, Governance und Projekte. Springer Vieweg.

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Hachette Book Group.

1 Anmerkung der Redaktion: Der vorliegende Artikel ist eine kondensierte Version der Masterarbeit von Frau Astrid Donaubauer-Grobner (siehe Literaturverzeichnis).

Das Thema automatische Gesichtserkennung bewegt nicht nur hierzulande die Gemüter. Das Versuchsprojekt von Bundesinnenministerium und Deutscher Bahn zur Gesichtserkennung am Berliner Bahnhof Südkreuz ist in guter Erinnerung. Die Kampagne „Reclaim your face" der NGO European Digital Rights (EDRi) war ein Meilenstein des Protests gegen den Versuch diese das Persönlichkeitsrecht Einzelner erheblich einschränkende Technik einzuführen. Interessant ist es, dass sich in der Volksrepublik China Widerstand regt gegen die Verwendung der Gesichtserkennung durch Unternehmen.

Lesen Sie darüber im englischsprachigen Beitrag von Frau Yu Du, Partnerin MMLC Group Lawyers & Consultants, Peking. Im Anschluss finden Sie eine Übersetzung, die wir mit Hilfe von deepl.com erstellt und dann so zu ändern versucht haben, dass die Übersetzung einigermaßen lesbar wird.

Yu Du

China's First Face Recognition Case Study

In 2019, Guo Bing, a professor of law at the Zhejiang Sci-Tech University, received a text message sent to consumers by Hangzhou Wildlife World Co., Ltd. (Wildlife World), indicating that consumers would enter the park, through face recognition, instead of fingerprint recognition. After failing to negotiate with Wildlife World on refund of the annual card, Guo Bing took Wildlife World to court. This case is known as the "first case of face recognition" in China, which has attracted widespread attention.

Case History

Guo Bing (Plaintiff) filed a lawsuit with Hangzhou Fuyang District Court on 28 October 2019 over the service contract dispute between him and Hangzhou Wildlife World Co., Ltd. (Defendant), requesting the court to 1) invalidate the Defendant's requirement on consumers' entrance to the park through fingerprint and facial recognition, 2) order the Defendant to return his actual card fee RMB1,360, 3) order the Defendant to compensate his transportation expenses RMB1,160 in total, 4) order the Defendant to delete all personal information (including but not limited to name, ID number, mobile phone number, photo, fingerprint data) submitted by the Plaintiff when he applied for the annual card and then used the annual card, under the witness of a third-party technical agency, at the Defendant's cost, and 5) order the Defendant to bear the litigation fee.

The Plaintiff claimed that the Defendant compulsorily required him to apply for and use the annual card through fingerprint entry, and after that, required him to register for face recognition, which violated the Consumer Rights Protection Law, and that the Defendant committed fraud in the process of providing services. Further, in accordance with the PRC Network Security Law, the Defendant's collection and use of consumers' personal information shall follow the principle of lawfulness, justification, and necessity", and shall not illegally collect and use personal information that is not related to its services.

The Defendant argued that when the Plaintiff applied for the annual card, the Defendant posted the application process, stating that the purpose of collecting information was to identify the identity of the actual card holders, which should have been informed by the Plaintiff, especially as a law professor specialist in personal information and data security, and based on this, the Plaintiff chose to agree to provide personal biometric information in exchange for the consumption discount of the annual card. The Defendant also argued that the Plaintiff had actually used fingerprint identification to enter the park many times, and during the performance of the service contract, the Defendant upgraded the recognition system to a facial feature recognition system, in order to solve the problem that the low recognition accuracy of the fingerprint machine caused the long queue time for annual card users to enter the park. Namely, the Defendant's collection and use of personal information were implemented with the consent of the Plaintiff, which complied with the provisions of the Consumer Protection Law and the PRC Civil Code. Further, the actual damage from the information disclosure had not yet occurred, but was just a hypothesis.

Court Decisions

The First Instance

Hangzhou Fuyang District Court held a hearing on 15 June 2020 and issued a decision on 20 November 2020. The court considered that the key point of this case is the evaluation and standardization of business operators' handling of consumers' personal information, especially personal biometric information such as fingerprints and human faces, and summarized the focus of the dispute in this case into the following three points:

1) The validity of the shop notices and text message notices claimed by Guo Bing

The Chinese laws do not prohibit the collection and use of consumers' personal information, but emphasize the supervision and management of the process of personal information processing. In this case, Wildlife World uses fingerprint and face recognition, based on the fact that annual card users can enter the park unlimited times during the validity period, to identify the identity of annual card users and improve the efficiency of entering the park for annual card users. Such act itself meets the requirements of the three principles of "lawfulness, justification, and necessity" stipulated by the Consumer Rights Protection Law. When Guo Bing applied for the annual card, the shop notice of Wildlife World informed in eye-catching form that some personal information including fingerprints of purchasers would be needed. Guo Bing decided to provide this information to be-

come a customer of the annual card. The content of the shop notice protected Guo Bing's right to know about consumption and the right to make independent decisions about personal information, but did not exclude or restrict consumers' rights, reduce or exempt operators' responsibilities, or increase consumer responsibilities that are unfair and unreasonable to consumers, which did not constitute any invalidity referred to in Paragraph 3 of Article 26 of the Consumer Rights Protection Law. Therefore, the court did not support Guo Bing's first claim.

In this case, when Guo Bing and Wildlife World had reached an agreement to adopt fingerprint identification to enter the park, Wildlife World sent Guo Bing two text messages during the performance of the contract, intending to change the originally agreed fingerprint identification into the face recognition, which is a unilateral change of the contract. From the perspective of the conclusion of the contract, the content of the text message is a new offer to Guo Bing. In view of the fact that Guo Bing had clearly stated before the lawsuit that he did not agree to enter the park through face recognition, and requested to confirm the invalidity of the two short messages by way of litigation, it should be determined that the aforementioned offer issued by Wildlife World has expired. The shop notice on face recognition posted by Wildlife World is mainly for unspecified users who newly apply for a card, so the shop notice has not become the contract clause between Guo Bing and Wildlife World, and has no legal effect on Guo Bing, namely, Guo Bing has no direct legal interest in the shop notice. His request to confirm the invalidity of the text message and shop notices involving facial recognition did not comply with the provisions of Item 1 of Article 119 of the Civil Procedure Law, and accordingly was not supported by the court.

2) Whether Wildlife World has breached the contract or fraud, and if so, how to determine the loss

Regarding the breach of contract and compensation claimed by Guo Bing, Wildlife World, without any consultation with Guo Bing and without his consent, sent a text message to inform Guo Bing that he would not be able to enter the park without registering face recognition. This behavior is an explicit indication of non-fulfilment of the original contract. According to Article 108 of the Contract Law, Guo Bing, as the observant party, is entitled to request Wildlife World to assume responsibility for breach of contract before the expiry of the performance period, including the loss of contract profits (RMB678) and partial transportation expenses (RMB360) from 26 October 2019 to the expiry date of the contract period.

Regarding the fraud and compensation claimed by Guo Bing, it is necessary and reasonable for Wildlife World to adopt differentiated inspection methods for different customer groups. The court believes that there is no evidence showing that Wildlife World deliberately concealed other ways of entering the park to mislead Guo Bing's consumption decision when applying for the card, so Guo Bing's such claim lacked basis. Further, Wildlife World used fingerprint recognition technology for legitimate business activities, and collected and used fingerprint information with the consent of consumers. There is no evidence showing that this technology and the tour services provided by Wildlife World do not meet the requirements of "guarantee personal and property safety", as referred to Paragraph 1 of Article 5 and Paragraph 1 of Article 16 of the Measures for the Punishment of Violations of Consumer Rights and Interests.

3) Whether Guo Bing can require Wildlife World to delete his personal information that has been collected

The court believes that this case is a service contract lawsuit, and the contract between Guo Bing and Wildlife World does not stipulate the deletion of personal information. Guo Bing's request for Wildlife World to delete his personal facial recognition information was supported by the court, since it was not necessary, however, his request for Wildlife World to delete other information than facial recognition, including name, ID number, fingerprint identification information, phone number, admission records, was not supported by the court.

Based on the above, the court ordered the Defendant to compensate the Plaintiff with a total of RMB1,038 for the loss of contract benefits and transportation expenses, and delete the facial feature information including photos submitted by the Plaintiff when he applied for the annual fingerprint card, within 10 days, and rejected the Plaintiff's other requests.

The Second Instance

Dissatisfied with the judgment of the first instance, Guo Bing and Wildlife World appealed to the Hangzhou Intermediate Court respectively. The intermediate court held a hearing on 29 December 2020, and issued the final decision on 9 April 2021. In the final decision, the court additionally ordered the Defendant to delete the Plaintiff's fingerprint information, in addition to the facial recognition information, and maintained the other judgement of the first instance.

Comments

Guo Bing told the news media after the final judgement that he was considering applying for a retrial, since the courts did not determine that Wildlife World's rules of fingerprint and face recognition as the only way to enter the park were invalid, nor supported that their deletion of his personal information should be done under the witness of a third-party technical agency. We will keep an eye to any process of this case. At the legislative level, China's existing laws only stipulate the general principles of lawfulness, fairness, and necessity for collection of personal information, and more detailed rules on special protection for face recognition information will be expected.

https://www.hg.org/legal-articles/china-s-first-face-recognition-case-study-58943

MMLC Group Lawyers & Consultants
1209 Tower W3, Oriental Plaza
One East Chang An Avenue
Beijing, People's Republic of China
北京铭辉达知识产权代理有限公司
北京东城区东长安街1号东方广场西
三办公楼1209室, 邮编100738
p +86 10 8515 1091, f +86 10 8515 1089
mmlcgroup.com

Ab hier folgt die deutsche Übersetzung des Artikels von Frau Yu Du (erstellt mit Hilfe von deepl.com):

Chinas erstes Gesichtserkennungs-Gerichtsverfahren

Im Jahr 2019 erhielt Guo Bing, Juraprofessor an der Zhejiang Sci-Tech University, eine SMS, die den Besuchern eines Wildparks geschickt wurde, die im Besitz einer Jahreskarte waren. In der SMS wurde darauf hingewiesen, dass die Verbraucher den Park in Zukunft nur nach einer Gesichtserkennung anstelle der bisher üblichen Fingerabdruckerkennung betreten würden. Nachdem die Verhandlungen mit Wildlife World über die Rückerstattung der Kosten der Jahreskarte gescheitert waren, verklagte Guo Bing Wildlife World vor Gericht. Dieser Fall ist als das „erste Gerichtsverfahren zur Gesichtserkennung" in China bekannt und hat große Aufmerksamkeit erregt.

Zum Fall

Guo Bing (Kläger) reichte am 28. Oktober 2019 beim Bezirksgericht Hangzhou Fuyang eine Klage im Zusammenhang mit einem Streit über einen Dienstleistungsvertrag zwischen ihm und Hangzhou Wildlife World Co. (Beklagte) ein und beantragte
1) die Anforderung der Beklagten, dass Verbraucher den Park nur nach Kontrolle per Fingerabdruck und Gesichtserkennung betreten könnten, für ungültig zu erklären,
2) die Beklagte zu verurteilen ihm seine tatsächliche Kartengebühr von 1.360 RMB zurückzuzahlen,
3) die Beklagte zu verurteilen seine Transportkosten von insgesamt 1.160 RMB zu erstatten,
4) das Gericht möge der Beklagten auferlegen alle persönlichen Daten (einschließlich, aber nicht beschränkt auf Name, Ausweisnummer, Mobiltelefonnummer, Foto, Fingerabdruckdaten), die der Kläger bei der Beantragung der Jahreskarte angegeben hatte und die während der Nutzung erhoben wurden, im Beisein einer dritten Partei (mit technischem Fachverstand) auf Kosten der Beklagten zu löschen und
5) die Beklagte zu verurteilen die Prozesskosten zu tragen.

Der Kläger behauptete, dass die Beklagte ihn zwang die Jahreskarte mittels Fingerabdruckeingabe zu beantragen und zu benutzen, und ihn danach aufforderte sich für die Gesichtserkennung zu registrieren, was gegen das Gesetz zum Schutz der Verbraucherrechte verstoße, und dass die Beklagte bei der Erbringung von Dienstleistungen arglistig gehandelt habe. Darüber hinaus müsse die Beklagte gemäß dem Netzsicherheitsgesetz der VR China bei der Erhebung und Nutzung der personenbezogenen Daten von Verbrauchern den Grundsatz der Rechtmäßigkeit, Korrektheit und Erforderlichkeit beachten und dürfe keine personenbezogenen Daten, die nicht im Zusammenhang mit ihren Dienstleistungen stehen, unrechtmäßig erheben und nutzen.

Die Beklagte argumentierte, dass die Beklagte, als der Kläger die Jahreskarte beantragte, den Antragsprozess veröffentlichte und darauf hinwies, dass der Zweck der Datenerfassung darin bestand die Identität der tatsächlichen Karteninhaber zu ermitteln, was dem Kläger, insbesondere als Juraprofessor, der auf persönliche Informationen und Datensicherheit spezialisiert ist, hätte erkennbar sein müssen, und dass sich der Kläger auf dieser Grundlage dazu entschloss im Austausch für den Verbrauchsrabatt der Jahreskarte persönliche biometrische Daten bereitzustellen. Die Beklagte argumentierte auch, dass der Kläger tatsächlich viele Male die Fingerabdruck-Identifikation für den Eintritt in den Park verwendet habe und dass die Beklagte während der Erfüllung des Dienstleistungsvertrags das Erkennungssystem auf ein System zur Erkennung von Gesichtsmerkmalen aufgerüstet habe, um das Problem zu lösen, dass die geringe Erkennungsgenauigkeit des Fingerabdruckgeräts die langen Wartezeiten für die Nutzer der Jahreskarte beim Eintritt in den Park verursacht habe. Die Erhebung und Verwendung personenbezogener Daten durch die Beklagte erfolgte tatsächlich mit der Zustimmung des Klägers, was den Bestimmungen des Verbraucherschutzgesetzes und des Zivilgesetzbuches der VR China entsprach. Außerdem war der tatsächliche Schaden durch die Weitergabe der Daten noch nicht eingetreten, sondern nur eine hypothetische Möglichkeit.

Gerichtsentscheidungen

Die erste Instanz

Das Bezirksgericht Hangzhou Fuyang hielt am 15. Juni 2020 eine Anhörung ab und erließ am 20. November 2020 eine Entscheidung. Das Gericht vertrat die Auffassung, dass der Kernpunkt dieses Falles die Bewertung und Standardisierung des Umgangs von Unternehmern mit personenbezogenen Daten von Verbrauchern, insbesondere mit biometrischen Daten wie Fingerabdrücken und Gesichtern, sei und fasste den Schwerpunkt des Rechtsstreits in diesem Fall in den folgenden drei Punkten zusammen:

1) Die Gültigkeit der von Guo Bing reklamierten Ladenbekanntmachungen und SMS

Die chinesischen Gesetze verbieten nicht die Erhebung und Verwendung personenbezogener Daten von Verbrauchern, sondern legen den Schwerpunkt auf die Überwachung und Verwaltung des Prozesses der Verarbeitung personenbezogener Daten. In diesem Fall verwendet Wildlife World die Fingerabdruck- und Gesichtserkennung auf der Grundlage der Tatsache, dass Jahreskartennutzer den Park während der Gültigkeitsdauer unbegrenzt oft betreten können, um die Identität der Jahreskartennutzer zu identifizieren und die Effizienz des Parkeintritts für Jahreskartennutzer zu verbessern. Eine solche Maßnahme erfüllt die Anforderungen der drei Grundsätze „Rechtmäßigkeit, Korrektheit und Erforderlichkeit", die im Gesetz zum Schutz der Verbraucherrechte festgelegt sind. Als Guo Bing die Jahreskarte beantragte, wies das Ladenschild von Wildlife World in auffälliger Form darauf hin, dass einige persönliche Daten, einschließlich der Fingerabdrücke des Käufers, benötigt würden. Guo Bing entschied sich diese Angaben zu machen, um Kunde der Jahreskarte zu werden. Der Inhalt des Hinweises im Geschäft schützte Guo Bings Recht über den Konsum Bescheid zu wissen und das Recht unabhängige Entschei-

dungen über persönliche Informationen zu treffen, schloss aber nicht die Rechte der Verbraucher aus oder schränkte sie ein. Er reduzierte oder befreite auch nicht die Verantwortung der Betreiber oder erhöhte die Verantwortung der Verbraucher, was unfair und unzumutbar wäre und stellte somit keine Ungültigkeit im Sinne von Artikel 26 Absatz 3 des Gesetzes zum Schutz der Verbraucherrechte dar. Daher gab das Gericht der ersten Klage von Guo Bing nicht statt.

In diesem Fall, in dem Guo Bing und Wildlife World eine Vereinbarung über die Identifizierung von Fingerabdrücken für den Zutritt zum Park getroffen hatten, schickte Wildlife World Guo Bing während der Vertragserfüllung zwei SMS mit der Absicht die ursprünglich vereinbarte Identifizierung per Fingerabdrücken durch eine Identifizierung per Gesichtserkennung zu ersetzen, was eine einseitige Vertragsänderung darstellt. Unter dem Gesichtspunkt des Vertragsschlusses ist der Inhalt der SMS ein neues Angebot an Guo Bing. In Anbetracht der Tatsache, dass Guo Bing vor dem Gerichtsverfahren eindeutig erklärt hat, dass er nicht damit einverstanden ist den Park über die Gesichtserkennung zu betreten, und beantragt hat die Ungültigkeit der beiden SMS auf dem Rechtsweg zu bestätigen, sollte festgestellt werden, dass das oben genannte Angebot von Wildlife World erloschen ist. Das von Wildlife World veröffentlichte Angebot zur Gesichtserkennung richtet sich in erster Linie an nicht näher bezeichnete Nutzer, die neu eine Karte beantragen, so dass das Angebot nicht zu einer Vertragsklausel zwischen Guo Bing und Wildlife World geworden ist und keine rechtlichen Auswirkungen auf Guo Bing hat, d. h. Guo Bing hat kein unmittelbares rechtliches Interesse an dem Angebot. Sein Antrag auf Bestätigung der Ungültigkeit der SMS und der Shop-Benachrichtigung mit Gesichtserkennung entsprach nicht den Bestimmungen von Artikel 119 Absatz 1 des Zivilprozessgesetzes und wurde daher vom Gericht nicht unterstützt.

2) Zum Vertragsbruch und zur Frage des Schadensersatzes, ob Wildlife World den Vertrag gebrochen hat oder betrügt, und wenn ja, wie der Schaden zu bestimmen ist

Was den Vertragsbruch und die von Guo Bing geforderte Entschädigung angeht, so hat Wildlife World ohne jegliche Rücksprache mit Guo Bing und ohne dessen Zustimmung eine SMS geschickt, um Guo Bing mitzuteilen, dass er den Park nicht betreten könne ohne sich mit einer Gesichtserkennung zu registrieren. Dieses Verhalten ist ein eindeutiger Hinweis auf die Nichterfüllung des ursprünglichen Vertrags. Gemäß Artikel 108 des Vertragsgesetzes ist Guo Bing als betroffene Partei berechtigt Wildlife World aufzufordern die Verantwortung für den Vertragsbruch vor Ablauf der Leistungsperiode zu übernehmen, einschließlich des entgangenen Vertragsgewinns (678 RMB) und der teilweisen Transportkosten (360 RMB) vom 26. Oktober 2019 bis zum Ablauf der Vertragsperiode.

Was den von Guo Bing geltend gemachten Betrug und die Entschädigung betrifft, so ist es notwendig und angemessen, dass Wildlife World differenzierte Kontrollmethoden für verschiedene Kundengruppen anwendet. Das Gericht ist der Ansicht, dass es keine Beweise dafür gibt, dass Wildlife World absichtlich andere Zugangsmöglichkeiten zum Park verschwiegen hat, um Guo Bing bei der Beantragung der Karte in die Irre zu führen, so dass Guo Bings Behauptung jeder Grundlage entbehrt. Darüber hinaus setzte Wildlife World die Technologie zur Erkennung von Fingerabdrücken für rechtmäßige Geschäftsaktivitäten ein und sammelte und verwendete die Fingerabdruckdaten mit der Zustimmung der Verbraucher. Es gibt keine Beweise dafür, dass diese Technologie und die von Wildlife World angebotenen Reiseleistungen nicht die Anforderungen an die „Gewährleistung der Sicherheit von Personen und Eigentum" gemäß Artikel 5 Absatz 1 und Artikel 16 Absatz 1 der Maßnahmen zur Ahndung von Verstößen gegen Verbraucherrechte und -interessen erfüllen.

3) Zur Löschung der personenbezogenen Daten

Das Gericht ist der Ansicht, dass es sich in diesem Fall um einen Rechtsstreit über einen Dienstleistungsvertrag handelt und dass der Vertrag zwischen Guo Bing und Wildlife World keine Löschung personenbezogener Daten vorsieht. Guo Bings Antrag auf Löschung seiner persönlichen Gesichtserkennungsdaten durch Wildlife World wurde vom Gericht unterstützt, da diese nicht zur Vertragserfüllung notwendig seien. Seinem Antrag auf Löschung anderer Daten als Gesichtserkennungsdaten, einschließlich Name, ID-Nummer, Fingerabdruck-Identifikationsdaten, Telefonnummer und Zulassungsunterlagen, wurde vom Gericht jedoch nicht stattgegeben.

Auf der Grundlage der obigen Ausführungen wies das Gericht die Beklagte an den Kläger mit insgesamt 1.038 RMB für den Verlust von Vertragsleistungen und Transportkosten zu entschädigen und die vom Kläger bei der Beantragung der Jahreskarte für Fingerabdrücke eingereichten Gesichtsdaten einschließlich Fotos innerhalb von 10 Tagen zu löschen, und wies die weiteren Anträge des Klägers zurück.

Die zweite Instanz

Da sie mit dem Urteil der ersten Instanz nicht zufrieden waren, legten Guo Bing und Wildlife World jeweils Berufung beim Zwischengericht in Hangzhou ein. Das Zwischengericht hielt am 29. Dezember 2020 eine Anhörung ab und erließ am 9. April 2021 die endgültige Entscheidung. In der endgültigen Entscheidung wies das Gericht die Beklagte zusätzlich zu den Gesichtserkennungsdaten an die Fingerabdruckdaten des Klägers zu löschen, und hielt das andere Urteil der ersten Instanz aufrecht.

Kommentar

Guo Bing erklärte gegenüber den Medien nach dem endgültigen Urteil, dass er erwäge die Wiederaufnahme des Verfahrens zu beantragen. Das Gericht habe nicht festgestellt, dass die Vorschriften von Wildlife World, wonach der Park nur nach Identifikation per Fingerabdruck und Gesichtserkennung betreten werden dürfe, ungültig seien. Das Gericht habe auch nicht befürwortet, dass die Löschung seiner persönlichen Daten unter dem Beisein einer dritten Partei (mit technischem Fachverstand) erfolgen sollte.

Wir werden den weiteren Verlauf dieses Falles im Auge behalten. Auf gesetzgeberischer Ebene sehen die bestehenden Gesetze Chinas nur die Beachtung der allgemeinen Grundsätze der Rechtmäßigkeit, Fairness und Erforderlichkeit für die Erhebung personenbezogener Daten vor. Man wird erwarten können, dass der Gesetzgeber der VR China künftig detailliertere Regeln für den Schutz von Gesichtserkennungsdaten schaffen wird.

Riko Pieper

Gefälschte Impfzertifikate?

Nach der Welle ist vor der Welle. Diese – in Anlehnung an Fußball-Fachwissen – auch auf die Corona-Infektionen übertragbare Weisheit, hat den Arbeitskreis Kryptografie (AK Krypto) des BvD[1] veranlasst sich einmal ein paar Gedanken zu den Impfzertifikaten und deren „Fälschungen" zu machen.

Seit es für Corona Impfstoffe gibt und Ungeimpfte mit Einschränkungen leben mussten, gab es auch zunehmend das Phänomen der gefälschten Impfpässe/Impfzertifikate. Sicher gab es auch schon vor der Pandemie derartige Fälle, aber diese spielten offensichtlich keine große Rolle. Zu einem massenhaften Anstieg von gefälschten Impfpässen kam es erst im Zusammenhang mit Corona und der Nutzung von digitalen Zertifikaten in der Corona-Warn-App (CWA) oder anderen Apps, in denen die digitalen Zertifikate gespeichert und angezeigt werden konnten.

Laut Robert Koch-Institut (RKI) wurden seit Beginn der Impfkampagne bis zum 27.01.2022 insgesamt rund 162,1 Millionen Dosen verimpft. Ausgestellt wurden aber 204,7 Millionen Zertifikate. Damit wurden rund 42,6 Millionen mehr Zertifikate ausgestellt als Impfungen verabreicht. Es gibt unterschiedliche Gründe, weshalb teilweise pro Impfung mehrere Zertifikate ausgestellt wurden. Das war aber wohl kaum bei ¼ der Impfungen der Fall. Die Anzahl der unberechtigten Impfzertifikate hat laut Medienberichten zum Jahresende 2021 extrem zugenommen. Die Diskrepanz zwischen Impfungen und Zertifikaten lag am 15.12.2021 „nur" bei etwa 25,8 Millionen und hat sich innerhalb weniger Wochen fast verdoppelt. Zunächst war auch nicht klar, ob derartige Fälschungen strafbar sind. Erst durch die Reform des Strafgesetzbuches wurde diese Lücke im Herbst 2021 geschlossen.

Aber: Was wurde eigentlich gefälscht? Handelt es sich hier tatsächlich um „Fälschungen"? Was hat das mit Kryptografie zu tun?

Die Antwort auf die letzte Frage sei hier vorweggenommen: Digitale Impfzertifikate sind elektronisch signiert und nach dem Stand der Technik somit fälschungssicher. Fälschen lässt sich zwar grundsätzlich alles (jede „0" kann in eine „1" geändert werden und umgekehrt), aber bei den verwendeten Verfahren, die zur elektronischen Signatur der Impfzertifikate eingesetzt werden, ist es nach derzeitigem kryptologischen Wissensstand nicht möglich eine Änderung durchzuführen, ohne dass diese Änderung bemerkt wird.

Das gilt jedenfalls für alle heutigen Computer in Kombination mit den hier verwendeten Algorithmen und Signierverfahren. Falls einmal in ein paar Jahren Quantencomputer zum Einsatz kommen, wird die Situation voraussichtlich anders sein. Wann es so weit ist, weiß man nicht genau. Allgemein geht man davon aus, dass es in den nächsten paar Jahren noch keine derartig nutzbaren Quantencomputer geben wird.

Ohne an dieser Stelle näher darauf einzugehen sei hier erwähnt, dass der Begriff der „elektronischen Signatur" oft missverstanden wird. Definiert ist er in der Verordnung (EU) Nr. 910/2014 (eIDAS-Verordnung)[2], welche unterschiedliche elektronische Signaturen vorsieht. Laut der Begriffsbestimmungen im Art. 3[3] Nr. 10 gilt:

„Elektronische Signatur" sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet.

Dieses Kriterium erfüllt bereits jede E-Mail, der der Name des Unterzeichners beigefügt ist. Ein derart ergänzter Name hat jedoch keinerlei Beweiskraft (dass wirklich die Person unterschrieben hat, deren Name angegeben ist, bzw. dass der Text nach dem Unterzeichnen nicht verändert wurde). Erst die „Fortgeschrittene elektronische Signatur" (Nr. 11 der Begriffsbestimmungen) erfüllt die oben genannten Kriterien und davon ist bei den Signaturen der Impfzertifikate die Rede.

Entsprechendes gilt für elektronisch Siegel (Nr. 25 der Begriffsbestimmungen), die auch für juristische Personen wie Behörden und Unternehmen und somit auch für Ärzte oder Apotheker ausgestellt werden können und bei den Impfzertifikaten zum Einsatz kommen. Der Unterschied soll aber keine Rolle spielen, denn technisch bzw. mathematisch oder kryptografisch gibt es hier keinen Unterschied zu den fortgeschrittenen Signaturen, so dass hier weiterhin von elektronischen Signaturen die Rede ist.

So, wie es die CWA (und andere Apps) gibt, in die man die Impfzertifikate über den darauf enthaltenen QR-Code einlesen und vorzeigen kann, gibt es auch das entsprechende Gegenstück: die „CovPass Check"-App.

Auch die „CovPass Check"-App wird (wie die CWA) vom RKI über die üblichen App-Stores kostenlos zur Verfügung gestellt. Mit diesen Apps können die QR-Codes der Impfzertifikate gelesen und geprüft werden. Die Daten der Impfzertifikate sind einschließlich der elektronischen Signatur im jeweiligen QR-Code eines Zertifikats enthalten.

Aufgrund der Berichterstattung hatte man den Eindruck, dass die Technik schuld ist bzw. die CWA oder die „CovPass Check"-App kaputt sei. Über das dazugehörige Prüfverfahren hingegen wurde kaum diskutiert. Ein Grund könnte sein, dass die elektronische Signatur als der kompliziertere Teil erachtet wurde.

Obwohl die Impfzertifikate zunächst auf Papier gedruckt werden, handelt es sich dabei um digitale Zertifikate, denn der QR-Code besteht mit seinen hellen und dunklen Punkten letzten Endes aus vielen „Nullen" und „Einsen". Der Datenträger (das Papier) kann also analog sein, aber die Information darauf (die Daten) sind trotzdem digital. Die Papierzertifikate können von den Apps eingelesen werden. Danach können die Zertifikate – insbesondere der QR-Code sowie weitere relevante Daten – auch



Bild: iStock.com / Claudia Nass

von der CWA angezeigt werden und es ist nicht erforderlich das Original des Papierzertifikats immer bei sich zu tragen. Üblicherweise hat man sein Smartphone immer dabei.

Falls aber jemand gar kein Smartphone besitzt, ist das auch kein Problem. In diesem Fall kann man das Original des Papierzertifikats oder auch eine Kopie davon bei sich tragen oder z. B. (was manche Apotheken anbieten) den QR-Code des Zertifikats auf eine Art Ausweiskarte drucken lassen. In allen Fällen ist es also möglich ein elektronisch signiertes Impfzertifikat immer bei sich zu haben – mit oder ohne Elektronik (Smartphone) – und dieses ist folglich auch verlässlich mit einer Prüf-App verifizierbar. Die in Deutschland hauptsächlich verwendete „CovPass Check"-App setzt dies vorbildlich um, inkl. Datenminimierung und Speicherbegrenzung.

Nachdem nun geklärt ist, warum die bei digitalen Impfzertifikaten genutzten elektronischen Signaturen fälschungssicher sind und dass Fälschungen von Impfzertifikaten, die nicht von den Apps CWA oder „CovPass Check"-App (wenn man sie nutzt) angezeigt werden, eigentlich nicht möglich sein sollten, stellt sich die Frage, was es denn mit den anfangs erwähnten vielen Fälschungen auf sich hat.

Die einfache Antwort: Die digitalen Impfzertifikate wurden nicht „gefälscht" (bestenfalls im juristischen Sinne, aber nicht aus Sicht der Kryptografie, die die Authentizität und Integrität eines signierten Dokuments sicherstellt), da dies nach dem aktuellen Stand der Technik nicht möglich ist.

Was aber möglich – und scheinbar auch einfach – ist, ist eine Fälschung des alten gelben analogen Impfpasses auf Papier. Der enthält zwar neben einem Stempel für jede Impfung auch eine Unterschrift und einen Aufkleber mit Angaben des jeweiligen Impfstoffes. Diese Angaben sind jedoch leicht zu fälschen bzw. die Echtheit ist schwer bzw. gar nicht zu überprüfen. Wenn man mit einem gefälschten Impfpass z. B. zu einer Apotheke geht und sich auf dieser Basis einen digitalen Impfpass ausstellen lässt, dann hat man aus einem gefälschten Impfpass ein „echtes" (weil nicht gefälschtes, sondern von einem „befugten"[4] Apotheker ausgestelltes und unverändertes) Impfzertifikat anfertigen lassen – wenn auch unrechtmäßig.

Eine weitere Möglichkeit ist, dass sich jemand als Arzt oder Apotheker ausgibt, der keiner ist und so unrechtmäßig ein Zertifikat zur Erstellung von Impfzertifikaten erwirbt. An dieser Stelle gab es offensichtlich Defizite bei der Überprüfung der Angaben des vermeintlichen Arztes/Apothekers. Solche unechten Ärzte/Apotheker konnten dann mit ihrem Zertifikat auch Impfzertifikate ausstellen.

Die Überprüfung eines solchen Zertifikats würde von der „CovPass Check"-App jedenfalls zunächst nicht beanstandet und das Zertifikat somit als „gültig" angezeigt werden. Das liegt daran, dass sowohl der angegebene Name und das Geburtsdatum mit dem des vorzulegenden Ausweises übereinstimmt (wenn das so auf dem gefälschten Papier-Impfpass eingetragen war), als auch die Zertifikatangaben nach der Signatur nicht mehr verändert wurden. Das ist mit handschriftlichen Unterschriften vergleichbar. Wenn jemand ein Dokument nach Vortäuschung falscher Tatsachen unterschreibt, dann ist das zwar nicht in Ordnung und auch anfechtbar, aber die Unterschrift wäre nicht gefälscht.

Eine andere Möglichkeit, sich unrechtmäßig ein „echtes" Impfzertifikat zu erschleichen, wäre den ausstellenden Verantwortlichen (z.B. Arzt, Apotheker) mittels einer geldlichen Zuwendung zu „überreden" dies zu tun.

Alle genannten Varianten hat es in der Vergangenheit gegeben. Bei der ersten Variante war es so, dass die gefälschten Impfpässe in großen Mengen über das Internet bzw. Darknet angeboten wurden. Das kann jedoch auch von Strafverfolgungsbehörden aufgedeckt und dann – jedenfalls für den konkreten Anbieter dieser Fälschungen – beendet werden. Bei der zweiten und dritten Variante fällt es auch irgendwann auf, wenn jemand zu viele unberechtigte Zertifikate ausstellt – z. B. weil jemand erwischt wurde, der sich definitiv nicht geimpft und dies evtl. auch stolz überall herumerzählt hat und trotzdem ein „gültiges" Zertifikat vorzeigen konnte ohne einen gültigen Eintrag in seinem Impfpass vorweisen zu können. In solchen Fällen kann man die elektronische Signatur der Verantwortlichen der ausgestellten Zertifikate für ungültig erklären und auf eine entsprechende Liste setzen. Damit wären dann ggf. alle Zertifikate dieses Verantwortlichen nachträglich ungültig.

Abschließend sei hier noch auf die zu lasche bzw. fatal falsche Überprüfung der Impfpässe hingewiesen:

Viele Nutzer der CWA haben wahrscheinlich schon erlebt, dass man sein (korrektes) Impfzertifikat einschließlich gültigem Personalausweis zum Einlass vorgezeigt hat und dann einfach durchgewunken wurde. Dabei war für den Prüfer oft nur der QR-Code per „Sichtprüfung" erkennbar. Es ist vollkommen schleierhaft, was diese „Prüfung" bringen soll, denn kein Mensch kann einen QR-Code mit bloßem Auge entziffern, dekodieren und auch noch die darin enthaltene elektronische Signatur überprüfen. Allein für die krypto-

grafische Überprüfung der Signatur sind sehr komplexe mathematische Operationen nötig, die kein Rechenkünstler, der mit dieser Nummer im Zirkus auftreten wollte, je bewerkstelligen könnte.

In anderen Fällen wurde der QR-Code auch noch etwas nach oben gescrollt, damit man (wenigstens) den Namen und das angegebene Geburtsdatum mit dem Ausweis vergleichen und auch den Impfstatus lesen konnte. Nach der Lektüre dieses Artikels sollte aber jedem klar sein, dass auch das nicht ausreichend ist, denn wenn man den QR-Code nicht mit einer App überprüft, dann kann darunter beliebiger Text stehen, ohne dass dieser als Fälschung erkennbar wäre.

Als Fazit bleibt festzuhalten:

Die Schwachstelle sind nicht die digitalen Impfzertifikate (QR-Code im Handy oder auf Papier), die über elektronische Signaturen kryptografisch abgesichert sind. Die Schwachstelle sind die analogen (gelben) Impfpässe, die keine hinreichenden Sicherheitsmerkmale aufweisen sowie die teilweise zu lasche Überprüfung der Ärzte/Apotheker, die ihr eigenes Zertifikat einschließlich der Möglichkeit zur Ausstellung von „signierten" Impfzertifikaten beantragen und die unbekümmerte und unzureichende – ja geradezu schildbürgerhafte – „Überprüfung" der Zertifikate.

1 Der vorliegende Text ist eine Zusammenfassung einer Diskussion der Mitglieder des AK Krypto des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V., die während eines Arbeitskreistreffens geführt wurde. Der Text wurde Ende August 2022 unter https://www.bvdnet.de/ak-krypto-zu-impfzertifikaten/ als Blogbeitrag veröffentlicht.

2 https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0910&from=DE sowie Erläuterung dazu bei Wikipedia: https://de.wikipedia.org/wiki/Verordnung_(EU)_Nr._910/2014_(eIDAS-Verordnung)

3 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32014R0910&from=DE#d1e810-73-1

4 Ob der Apotheker immer „befugt" ist oder die Befugnis ggf. unrechtmäßig erworben wurde, wird weiter unten thematisiert.

Heinz Alenfelder

Eine Milliarde Matrixcode-Briefmarken – Was steckt dahinter?

Ende Mai 2022 verkündete die Deutsche Post AG stolz, dass sie fünfzehn Monate nach Einführung des neuen Matrixcodes auf Postwertzeichen bereits eine Milliarde dieser Briefmarken verkauft habe. Verschiedene Zeitungsartikel informierten entlang des Presseerklärungstextes. Dieser Beitrag soll die Hintergründe zusammentragen ohne weiter auf die Einhaltung des Postgeheimnisses (Artikel 10 des Grundgesetzes) einzugehen, die schlicht vorausgesetzt werden muss.

Das Grundsätzliche

Seit diesem Jahr tragen sämtliche von der Deutschen Post herausgegebenen Briefmarken zusätzlich zum Motiv einen Matrixcode. Dieser Code darf nicht abgeschnitten werden, denn er soll die Briefmarken fälschungssicher machen. Dazu wird jedes auf einem Brief verwendete Postwertzeichen beim Sortieren im Briefzentrum nicht nur per Stempelaufdruck entwertet, sondern auch digital erfasst. Wenn die Briefmarke bereits erfasst sein sollte, also bereits zum Frankieren benutzt wurde, beziehungsweise wenn es sich um eine Kopie oder Fälschung handelt, wird der Brief nicht befördert, sondern an den Absender zurück gesendet.

Über den gescannten Matrixcode einer Briefmarke können mit der Post-App jederzeit – auch nach dem Empfang des Briefs – zusätzliche Informationen zur Briefmarke selbst abgerufen werden. Im Rahmen der kostenlosen Basis-Sendungsverfolgung wird als Zusatznutzen abrufbar, wann der Brief im Start-Briefzentrum bearbeitet wurde und wann er im Briefzentrum der Zielregion angekommen ist. Voraussetzung dafür ist das Scannen der Marke vor dem Versand. Die Zustellung selbst wird explizit nicht protokolliert, dazu ist eine Extragebühr für ein Einschreiben nötig.

Die Details

Auf ihrer Webseite erläutert die Deutsche Post („Wissenswertes über den Matrixcode in der Frankierung"[1]), dass sie den „DataMatrix-Code" in unterschiedlichen Größen und Formen einsetzt. Demnach enthält er auf den Briefmarken folgende Daten:

- Die Buchstaben „DEA", um das Land (DE - internationale Kennzeichnung Deutschland) und die Transportfirma zu kennzeichnen (A - Deutsche Post).
- Die Art der Frankierung, hier also, dass es sich um ein Postwertzeichen handelt.
- Eine laufende Nr. je Motiv als eindeutiger Zähler sowie eine interne Nummernkreiskennung, die eine Auflage bzw. ein Motiv angibt und eine Kennung für das Motiv, das die Briefmarke zeigt.
- Welche Druckerei dieses Postwertzeichen gedruckt hat und um welche Art es sich handelt, also ob es eine nassklebende oder selbstklebende Marke ist, die vom Bogen oder von der Rolle kommt.
- Weiterhin werden Informationen zur Absicherung der Echtheit und Fälschungssicherheit des Matrixcodes gespeichert. Dies ist der sog. Crypto-


Bild: Frans Valenta

string, ergänzt um einen Hash-Wert, wie er analog bei einer digitalen Signatur errechnet wird.
- Dann folgen schließlich das Ausgabedatum und der Wert der Briefmarke.

Diese Daten kann nur die Post auslesen. Für Briefmarken, die von Firmen selbst gedruckt werden können, gibt es allerdings entsprechende Scanner (z.B. für die Frankierung von Retouren zum späteren automatischen Verarbeiten). Zu weiteren technischen Details des Datamatrix-Codes auf Briefmarken, insbesondere zu den Vorteilen für Briefmarkensammler, äußert sich Jürgen Olschimke auf seiner Webseite[2].

Nach dem Scannen bei der Versandabwicklung der Briefe speichert die Post die Daten aus dem Matrixcode teilweise, um erkennen zu können, ob die Briefmarke bereits benutzt wurde. Außerdem ermöglicht der Matrixcode – wenn er vor dem Versand mit der Post-App gescannt wurde – die Verfolgung des Briefs bis zum Ziel-Briefzentrum. Dazu heißt es auf der Webseite der Post: „Es werden nur die für die Sendungsverfolgung relevanten Daten gespeichert, also die im Matrixcode enthaltene Sendungsnummer, Informationen zur Bearbeitung im Logistikzentrum und die auf der Sendung enthaltene Postleitzahl des Empfängers. Weitere Angaben wie Name oder Adresse von Absender oder Empfänger werden nicht gespeichert. Die Daten werden nach einer Frist von 21 Tagen automatisch gelöscht." Nicht angezeigt wird beispielsweise das Ziel-Briefzentrum, wenn die Empfängerin oder der Empfänger einen Nachsendeantrag gestellt hat, so dass der Umzug auf diese Weise nicht nachverfolgt werden kann. Abhängig von einer sog. Zusatzleistung (also Einschreiben, Nachnahme etc.) werden weitere Daten gespeichert, die über die „ordnungsgemäße Leistungserbringung" durch die Deutsche Post informieren.

Der Datenschutz

Um nun festzustellen, welche Bedingungen für die Daten gelten, die in Kombination mit dem Lesen von Absende- und Empfangs-Adresse eines Briefes im Rahmen der Sortierung gespeichert werden, ist ein Blick in die Datenschutzinformationen auf der Webseite der Deutschen Post AG[3] nötig. Die Post betont, dass natürlich das Postgeheimnis und auch das Postgesetz Anwendung finden und dass der Matrixcode nicht dazu diene Sendungsbeziehungen zwischen Personen auszuwerten. Ansonsten ist es nicht ganz einfach die Briefversand-Bedingungen aus der Vielzahl der Unterabschnitte der Datenschutzinformationen herauszufiltern.

Zunächst einmal treffen einige Punkte von „A. Allgemeiner Teil" auf den Briefversand zu, doch muss beim Lesen entschieden werden, worauf die Post die Datenverarbeitung wohl stützt. Als ein Grund wird genannt: „beispielsweise, um … Ihnen – sofern zulässig – bedarfsgerechte Werbung zukommen zu lassen". Fraglich ist also, ob das Zukommenlassen von Werbung aufgrund einer App-Nutzung zum Scannen des Matrixcodes zulässig wäre und ob es überhaupt stattfindet. Die Überprüfung der Briefmarke fällt wohl unter den Punkt „zu Zwecken der Entgeltsicherung".

Der Teil „B. Datenverarbeitung" bezieht sich auf die verschiedenen Online-Angebote von der Webseite über den Portokalkulator und die Sendungsnachverfolgung bis zur App und den sozialen Kanälen.

Schließlich geht der Teil „C. Produkte und Services" dann auf Briefsendungen ein. Dort entspricht sowohl die Art der Daten als auch die Liste der Verarbeitungszwecke den Erwartungen. Wiederum taucht hier der Begriff der bedarfsgerechten Werbung auf, diesmal mit einem Link zu einem Kontaktformular für diejenigen, die von „Widerspruchsrechten – insbesondere gegen die Verwendung Ihrer Daten zu Werbezwecken – Gebrauch machen möchten". Bei der Speicherdauer ist zwar bemerkenswert, dass es hier für nicht nachweispflichtige Sendungen heißt: „Daten … werden zwecks Qualitäts- und Entgeltsicherung bzw. wegen Erfüllung beauftragter Zusatzleistungen maximal 15 Werktage gespeichert". Daraus ist aber abzuleiten, dass die an anderer Stelle genannten 21 Tage für die Briefmarken-Daten selbst ohne die personenbezogenen Adress-Daten gelten. Jedenfalls wird die längere Speicherdauer auf Nachfrage durch einen Datenschutzberater der Deutschen Post AG mit „Serviceaspekt für den Kunden" begründet und als „ausgewogen und angemessen" bewertet.

Bezüglich der Basis-Sendungsverfolgung per „Post & DHL App" ist noch zu erwähnen, dass für diese App keine Registrierung nötig ist, wenn nicht mehr als 10 Sendungen gleichzeitig verfolgt werden sollen. Zur Beurteilung des Datenschutzverhalten der App sei abschließend auf Mike Kuketz verwiesen, der die „Post & DHL App" in seinem Blog im Oktober 2021 unter die Lupe genommen hat[4].

1 https://www.deutschepost.de/de/f/frankierung/matrixcode.html

2 http://jolschimke.de/briefmarken-und-ganzsachen/der-datamatrixcode-auf-briefmarken.html

3 https://www.deutschepost.de/de/f/footer/datenschutz.html

4 https://www.kuketz-blog.de/post-dhl-app-datenuebermittlung-an-tracking-anbieter-noch-vor-zustimmung-einwilligung/

Offener Brief anlässlich der Frühjahrskonferenz der Innenminister und -senatoren vom 30. Mai 2022

Vorratsdatenspeicherung in Deutschland und der EU stoppen: Ein Ende für die anlasslose Massenüberwachung


Bild: iStock.com / gorodenkoff

An die
Konferenz der Innenminister und -senatoren
Bundesinnenministerin Nancy Faeser

Es ist nun mehr als zehn Jahre her, dass zehntausende Menschen in Berlin und anderen Städten gegen die Vorratsdatenspeicherung auf die Straße gegangen sind. In verschiedenen Gerichtsentscheidungen wurde sie seither für europarechts- und verfassungswidrig erklärt. Denn die anlasslose und flächendeckende Speicherung der Telefon-, Internet- und Ortsdaten von Millionen von Bürgerinnen und Bürgern ist mit den Grundwerten einer freien und offenen Gesellschaft nicht zu vereinbaren.

Der späten Einsicht folgend, dass jeder Versuch einer grundrechtskonformen Massenüberwachung in einer Sackgasse enden muss, hat die Bundesregierung in ihrem Koalitionsvertrag beschlossen die anlasslose Vorratsdatenspeicherung endlich durch eine rechtssichere und anlassbezogene Lösung zu ersetzen. Konkrete Pläne, wie dieses Versprechen an die Bürgerinnen und Bürger umgesetzt werden soll, wurden aber leider bislang nicht vorgelegt.

Eine grundrechtsorientierte Sicherheitspolitik darf nicht immer wieder versuchen die Grenzen des gerade noch verfassungsmäßigen auszureizen. Eine solche Politik führt nicht nur zu einer sukzessiven Aushöhlung rechtsstaatlicher Grundsätze, sondern in der Praxis auch zu jahrelangen Hängepartien, in denen die Rechtslage weder für die Bürgerinnen und Bürger noch für die Sicherheitsbehörden nachzuvollziehen ist.

Wir sehen mit großer Sorge, wie Regierungen einiger europäischer Staaten die Rechtsprechung des EU-Gerichtshofs seit Jahren nicht umsetzen und stattdessen Gesetze schaffen, die in entscheidenden Punkten nicht den Anforderungen des EU-Rechts auf Schutz der Privatsphäre der Bürgerinnen und Bürger entsprechen. Diese Gesetze verstoßen teilweise gegen europäisches Recht und führen in der Praxis zu einer Massenüberwachung der Bevölkerung, die der EuGH wiederholt ausdrücklich verboten hat. Daran ändern auch Konzepte wie die geografisch „gezielte Vorratsdatenspeicherung", der pauschale Verweis auf die „nationale Sicherheit" oder die generelle Vorratsdatenspeicherung von IP-Adressen nichts.

Wir fordern Sie daher auf dem Spuk der Vorratsdatenspeicherung und dem unwürdigen Gezerre vor den Gerichten endlich ein Ende zu bereiten und sich auf nationaler wie europäischer Ebene für ein endgültiges Ende der grundrechtswidrigen Massenüberwachung einzusetzen.

Aktion Freiheit statt Angst
Electronic Frontier Finland
Elektronisk Forpost Norge [Norwegen]
epicenter.works [Österreich]
European Digital Rights (EDRi)
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIFF)
Deutsche Vereinigung für Datenschutz (DVD)
Deutscher Journalisten-Verband (DJV)
Digitale Gesellschaft
Digitalcourage
Homo Digitalis [Griechenland]
IT-Pol [Dänemark]
Republikanischer Anwältinnen- und Anwälteverein (RAV)

Pressemitteilung der DVD vom 15.08.2022

DVD: Online-Registerveröffentlichungen verstoßen gegen Datenschutz

Seit dem 1. August 2022 sind auf der Plattform „handelsregister.de“ sämtliche Einträge in den Handels-, Genossenschafts-, Partnerschafts- und Vereinsregistern über das Internet ohne weitere Einschränkungen abrufbar. Dadurch sind teilweise sensible persönliche Daten – Geburtsdaten, Adressen, Bankverbindungen, sogar Unterschriften z.B. von Vereinsvorständen oder von Unternehmensangehörigen – für jedermann online abruf- und auswertbar. Die Deutsche Vereinigung für Datenschutz e.V. (DVD) weist darauf hin, dass diese aktuelle Praxis zum Datenmissbrauch geradezu einlädt und fordert eine Bereinigung der Register um sensible Daten und eine Korrektur der Rechtsgrundlagen.

Die Online-Zugänglichkeit von Registern verfolgt das begrüßenswerte Ziel von mehr Transparenz im Wirtschaftsleben. Damit wird der europarechtlichen Verpflichtung der Digitalisierungs-Richtlinie ((EU) 2019/1151) entsprochen. In dieser Richtlinie wird in Art. 161 aber unmissverständlich klargestellt, dass bei der Umsetzung die EU-Datenschutz-Grundverordnung beachtet werden muss. Dies bedeutet, dass auch bei der Verwirklichung von öffentlichen Interessen – hier der Wirtschaftstransparenz – schutzwürdige Interessen der Betroffenen beachtet werden müssen. Statt dies korrekt umzusetzen, hat es sich die deutsche Verwaltung einfach gemacht und die früheren dezentralen und bisher nur mit Aufwand zugänglichen Register – eins-zu-eins – ins Internet gestellt. Damit wird ein explizites Ziel der EU-Digitalisierungs-Richtlinie – die Verhinderung von Identitätsdiebstahl – konterkariert: Die teilweise sensiblen Daten können dazu verwendet werden sich online als andere Person auszuweisen, eignen sich zur Einrichtung von Fake-Accounts, Fake-Bestellungen und zu anderen kriminellen Machenschaften bis hin zu persönlichen Bedrohungen. Zur Zuordnung von wirtschaftlichen Verantwortlichkeiten sind diese sensiblen Informationen regelmäßig nicht erforderlich. Nicht nur das: Der Bundesgesetzgeber hat unter dem Vorwand der Umsetzung der DSGVO – etwa im Bereich des Vereinsregisters (§ 79a BGB) – die datenschutzrechtlichen Betroffenenrechte wie z.B. den spezifischen Anspruch auf Auskunft oder auf Widerspruch ausgeschlossen.

DVD-Vorsitzender Frank Spaeing erläutert: „Gerade beim Vereinsregister werden mit der Online-Veröffentlichung viele Menschen gefährdet. Es wäre fatal, wenn durch die unbedachten Veröffentlichungen diese von ihrem besonderen ehrenamtlichen Engagement abgeschreckt würden.“ DVD-Vorstandsmitglied Thilo Weichert ergänzt: „Die alte Bundesregierung hat die DSGVO in vieler Hinsicht unter Missachtung der europarechtlichen Vorgaben umgesetzt. Eine zeitnahe Korrektur ist dringend nötig. Um kurzfristig den Missbrauch der Online-Daten zu verhindern, sollte den Betroffenen zumindest ein Widerspruchsrecht bzgl. der Registerveröffentlichung besonders sensibler Einzelangaben eingeräumt werden.“ DVD-Vorsitzender Frank Spaeing fordert: „Bis die Registerauskunft datenschutzkonform umgesetzt ist, muss die Online-Plattform abgeschaltet oder zumindest im Zugang wieder beschränkt werden.“

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Registerveröffentlichung mit sensiblen Daten

Auf der zentralen Registerplattform des Bundes „handelsregister.de" lassen sich seit dem 01.08.2022 sämtliche Einträge im Handels-, Genossenschafts-, Partnerschafts- und Vereinsregister per Webformular ohne weitere Beschränkungen abrufen. Die für die Allgemeinheit nun leicht zugänglichen Dokumente enthalten oft sensible persönliche Daten wie Adressen, Geburtsdaten, Bankverbindungen oder auch Unterschriften.

Bisher musste man sich für Auskünfte beim Portalbetreiber Amtsgericht Hamm per Fax registrieren und für viele Dokumente auch Gebühren entrichten. Das Portal diente bisher als zentrale Onlineauskunft der deutschen Registergerichte. Auf Grundlage des Gesetzes zur Umsetzung der Digitalisierungsrichtlinie der EU, dessen Umsetzungsfrist am 01.08.2022 ablief, wurde die Registerauskunft vereinheitlicht und die Zugangsbeschränkungen entfielen. Mit der Richtlinie will die EU die Gründung von Gesellschaften und die Verfügbarkeit von Registerinformationen vereinfachen.

Ein Portal, in dem jeder Bürger mal schnell nachsehen kann, wer hinter einem bestimmten Unternehmen oder einem Verein steht, ist für die Transparenz förderlich. Doch scheint man sich bei der Umsetzung wenig Gedanken zum Datenschutz gemacht zu haben: Vielen Datensätze enthalten private Daten oder Daten mit Missbrauchspotenzial.

So sind in etlichen Dokumenten Unterschriften nicht geschwärzt. Es finden sich private Anschriften im Klartext, häufig werden Geburtstage genannt. Bei Schriftsätzen von Vereinen sind auch im Klartext persönliche Kontonummern enthalten und bei Bestätigungen von Notaren sind zum Teil die Verifikationsnummern des Personalausweises enthalten.

Die für das Portal – das vom Justizministerium Nordrhein-Westfalen betrieben wird – zuständige Datenschutzbehörde, die Landesbeauftragte für Datenschutz und Informationsfreiheit (LDI NRW), betonte, dass es das Portal schon länger gibt. Neu sei nur, „dass Abrufe aus dem Register nicht mehr kostenpflichtig sind und keine Nutzerregistrierung mehr vorgesehen ist." Die LDI NRW verweist auf die rechtlichen Grundlagen, die sich aus einer Reihe von Paragrafen unter anderem des Handelsgesetzbuches (HGB) und der Handelsregisterverordnung ergeben. Insbesondere betont die Behörde unter Verweis auf Paragraf 10a HGB, das Portal diene „der Transparenz im Rechtsverkehr und der damit verbundenen Wirkungen gegenüber Dritten. Daher finden die Rechte nach der Datenschutzgrundverordnung grundsätzlich nur sehr eingeschränkt Anwendung." Sie sieht, dass der neue Zugang zum Handelsregister „eine höhere Sensibilität bei den Betroffenen ausgelöst hat, die sich um einen möglichen Missbrauch ihrer Daten sorgen" und regt daher an rechtliche Einschränkungen der freien Veröffentlichung aller Registerdaten im Netz im Interesse des Schutzes der betroffenen Personen zu erwägen, soweit europarechtliche Vorgaben dem nicht entgegenstehen.

Das Missbrauchspotenzial ist offensichtlich. Die Sicherheitsexpertin und „Krawall-Influencerin" Lilith Wittmann kündigte an eine Programmierschnittstelle (API) für das Handelsregister-Portal zu bauen, mit der einfach und schnell viele – auch sensible – Inhalte aus dem Portal abgerufen werden können.

Der Justiziar und Datenschutzbeauftragte des Heise-Verlags Joerg Heidrich erklärte: „Ich halte das für ein krasses Versagen des Gesetzgebers bei der Abwägung zwischen berechtigten Forderungen nach Transparenz auf der einen und den Rechten der Betroffenen auf der anderen Seite." Das Portal sei gut mit dem Domain-Register vergleichbar, meint Heidrich: „Dort sind die Einträge ja auch nicht öffentlich einsehbar und nur ausnahmsweise mit berechtigtem Interesse abrufbar. Warum die Ungleichbehandlung?" (Bager, Handelsregister.de: Onlineabfrage verrät private Daten, www.heise.de 05.08.2022, Kurzlink: https://heise.de/-7202516), dazu auch: Pressemitteilung der DVD auf der vorigen Seite.

Bund

BfDI leitet Verfahren wegen behördlicher Facebook-Fanpage ein

Der Bundesbeauftragte für den Datenschutz (BfDI), Ulrich Kelber, hat am 03.06.2022 dem Bundespresseamt (BPA) ein Anhörungsschreiben zukommen lassen, in dem die Behörde Stellung nehmen soll zu der Fanpage, die sie für die Bundesregierung auf Facebook betreibt. Knapp ein Jahr zuvor hatte der BfDI die Bundesbehörden aufgefordert ihre Facebook-Fanpages abzuschalten, da diese nicht datenschutzkonform betrieben werden könnten. Dabei kündigte er an ab Januar 2022 die Nutzung von Facebook-Fanpages durch die Bundesbehörden prüfen zu wollen. Gespräche mit dem Bundespresseamt und Facebook haben nach Angaben von Kelbers Behörde zu keiner Lösung der datenschutzrechtlichen Probleme geführt.

Der BfDI hatte bereits in einem Rundschreiben an die Ministerien und Behörden im Mai 2019 darauf hingewiesen, dass ein datenschutzkonformer Betrieb einer Facebook-Fanpage zurzeit nicht möglich sei. Öffentliche Stellen mit einer solchen Fanpage müssten mit Facebook „eine Vereinbarung zur gemeinsamen Verantwortlichkeit schließen, die den Anforderungen von Art. 26 Datenschutz-Grundverordnung (DSGVO) entspricht". Daraufhin hätten einzelne Ressorts, die

Fanpages betreiben, geantwortet, dass sie diese als ein wichtiges Element ihrer Öffentlichkeitsarbeit ansehen. Mit Datum vom 30.03.2022 untermauerte Kelber seine Ansichten mit einem Gutachten der Datenschutzkonferenz (DSK) zur (fehlenden) datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages. Zuvor – im Jahr 2011 (!) – hatte schon das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) versucht öffentlichen und nicht-öffentlichen Stellen den Betrieb von Facebook-Fanpages zu untersagen. Nach einer Odyssee über sechs Gerichts-Instanzen einschließlich des Europäischen Gerichtshofs (EuGH) obsiegte das ULD letztlich beim Oberverwaltungsgericht Schleswig-Holstein mit Urteil vom 25.11.2021 (Az 4 LB 20/13) ohne aber eine rechtliche Handhabe gegen den Weiterbetrieb der Fanpages in die Hand zu bekommen.

Kelber hatte abgewartet, wie die Verhandlungen mit dem BPA ausgehen. Facebook habe dem BPA nur das öffentlich bekannte „Addendum“ von Oktober 2019 übersandt; das ist nach Ansicht vom Kelber unzureichend. Wegen des ungenügenden Addendums hatte die grüne Bundestagsfraktion Facebook verklagt und Auskunft sowie eine umfassende Vereinbarung eingefordert. Das angerufene Landgericht Hamburg erklärte sich dreieinhalb Jahre nach Klageerhebung aber mit Urteil vom 17.05.2022 für unzuständig. Zuständig seien die Gerichte in Irland, wo Facebook seine europäische Hauptniederlassung hat (Az. 307 O 285/18).

Der BfDI beruft sich u.a. auf den EuGH, der in seinem Urteil vom 16.07.2020 zum Privacy Shield (DANA 3/2020, 199 ff.) klargestellt hat, dass personenbezogene Daten von EU-Bürgern nur an Drittstaaten außerhalb des Europäischen Wirtschaftsraums übermittelt werden dürfen, wenn sie dort gleichwertigen Schutz genießen wie in der EU. Für die USA hat er ein solches angemessenes Schutzniveau verneint; dort hat Facebook seinen Sitz.

Eine Anhörung ist die erste Stufe in einem förmlichen Aufsichtsverfahren. Der BfDI erläuterte: „Das Gesetz regelt hierzu keine starre Frist.“ Stattdessen können die Fristen für die Anhörung durch die Fachreferate des BfDI bestimmt werden, in der Regel betragen sie einen Monat. Die dann eingegangene Stellungnahme wird geprüft, anschließend entscheidet der BfDI, ob eine verwaltungsrechtliche Aufsichtsmaßnahme notwendig ist. Das kann ein Verbot der Verarbeitung von Daten oder ihrer Übermittlung an einen Empfänger in einem Drittland sein. Nach § 43 BDSG sind Geldbußen gegen Behörden und sonstige öffentliche Stellen ausgeschlossen. Anders als bei Unternehmen kann der BfDI nach einer Anfechtungsklage einer Behörde gegen eine Aufsichtsmaßnahme keinen sofortigen Vollzug anordnen. Das heißt, dass sich die Angelegenheit noch lange Zeit hinziehen kann (Wilkens, Facebook-Fanpage: Datenschutzbeauftragter eröffnet Verfahren gegen Bundesbehörde, www.heise.de 06.06.2022, Kurzlink: https://heise.de/-7132768).

Bund

Behördliche Kontendatenabrufe steigen weiter

Die Zahl der Kontendatenabrufe zur Ermittlung von Steuervergehen und anderen säumigen Zahlern durch Finanzämter, Sozialbehörden und Gerichtsvollzieher ist in den vergangenen Jahren kontinuierlich gestiegen und hat laut Bundesfinanzministerium im Jahr 2021 1,14 Mio. Kontenabrufe erreicht. Davon entfiel der größte Teil mit insgesamt 853.317 oder 85% der Abfragen auf Vollstreckungsverfahren. Die Finanzämter führten 146.344 Abrufe durch. Die Zahl der Anfragen durch Polizei- und Verfassungsschutzbehörden lag 2021 bei knapp 1000. Gemäß der Antwort der Bundesregierung auf eine Anfrage der CDU/CSU-Bundestagsfraktion (BT-Drs. 20/2751) überschritt die Anzahl der Anfragen 2020 erstmals knapp die Millionengrenze, 2019 waren es 915.257 Fälle.

Die Unionsfraktion stellte in ihrer Anfrage „Fragen zur Verhältnismäßigkeit und Rechtfertigung“ des gesamten Verfahrens angesichts der annähernden Vervierfachung der Abrufzahlen seit 2015. Unter ihrer Regierungsbeteiligung wurde das 2005 von Rot-Grün eingeführte Verfahren auf Gerichtsvollzieher ausgeweitet. Mittlerweile können diese Einblicke in die Stammdaten bei säumigen Gläubigern schon bei Summen unter 500 € erfolgen. Die Bundesregierung räumt ein keine Erkenntnisse über die mit den Kontenabfragen erzielten Ergebnisse zu haben. Das Bundeszentralamt für Steuern führt die Kontenabfragen zentral durch und gibt die Daten an die legitimierten Behörden in den Bundesländern weiter. Diese teilen dem Bund nicht ihre Ergebnisse mit. Daher könne die Bundesregierung „keine Aussage“ zum Verhältnis der Abfragefallzahlen zum Ergebnis der Verfahren treffen.

Laut der Bundesregierung sind 2021 für Verfahrenspflege und Modernisierung Kosten von 993.331 € angefallen. Dafür habe das IT-Dienstleistungszentrum des Bundes zudem 909 interne Personentage verbucht, was weitere 334.893 € ausmache. Dazu kommen die Kosten für die mit den Verfahren beschäftigten Mitarbeiter. Informationen über die Höhe der Erträge, die sich aus eventuellen Ermittlungserfolgen aufgrund einer Kontenabfrage ergaben, lägen nicht vor. Der Bundesdatenschutzbeauftragte Ulrich Kelber sah die jährlich rasant wachsende Nachfrage schon 2020 kritisch: Jeder Kontenabruf sei ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung. Der Datenschützer bezweifelte, ob das Werkzeug noch verhältnismäßig eingesetzt werde, und forderte die Bundesregierung nachdrücklich auf das Instrument zu evaluieren (DANA 2/2020, 114; Krempl, Gläserner Bankkunde: Über eine Million behördlicher Kontenabfragen, www.heise.de 26.07.2022, Kurzlink: https://heise.de/-7190523).

Bundesweit

Datenschützer planen Initiative gegen Adresshandel

Die hiesige Direktmarketing-Branche ist über ein Vorhaben der Datenschutzbeauftragten von Bund und Ländern beunruhigt eine klare gemeinsame Ansage gegen den hinter vielen zielgerichteten postalischen Kundenansprachen stehenden Adresshandel vorzunehmen. Eine große Mehrheit der deutschen

Aufsichtsbehörden, mehr als zehn von ihnen, sehen dabei die Datenschutz-Grundverordnung (DSGVO) auf ihrer Seite.

Baden-Württembergs Datenschutzbeauftragter, Stefan Brink, meinte, viele Bürger wollten „eben nicht mehr mit unerwünschter, nicht angeforderter sogenannter Verbraucherinformation konfrontiert und belästigt werden". Die DSGVO sehe vor, dass Konsumenten informiert werden müssen, wenn ihre Adresse verkauft wird. Sie müssten ausdrücklich in diese Praxis einwilligen: „Informiert heißt in diesem Zusammenhang, dass sie unaufgefordert und vorab darüber aufgeklärt werden müssen, wer welche Informationen zu welchen Zwecken haben möchte und ob dabei auch personenbezogene Daten wie Adressdaten weitergegeben werden sollen und wie lange sie genutzt werden sollen." Diese Aufklärungspflicht sei „eine echte Hürde." Hier müsse nun jeder, „der Adresshandel betreiben will, richtig liefern. Der Verbraucher muss das Recht haben werbefrei zu leben." Nach Ansicht der Datenschützer wissen die Empfänger von Werbeschreiben oft nicht, wer alles ihre Anschrift und nicht ganz so geheime Vorlieben kennt und wofür diese Informationen genutzt werden.

Die Datenschutzbeauftragten wollen offenbar die umstrittene Praxis weitgehend untersagen. Die Berliner Datenschutzbehörde ließ gemäß Presseberichten durchblicken, man arbeite an einem Beschluss, um bundesweit einheitlich aufzutreten. Dem stünden im Grunde nur noch die Kollegen in Nordrhein-Westfalen entgegen. Diese hielten den Adresshandel in der bisherigen Form weiter für zulässig. In dem Bundesland sitzen mit Tochterfirmen von Bertelsmann und der Deutschen Post zwei der größten deutschen Branchenvertreter. Das Treiben von Post Direkt im Bundestagswahlkampf 2017 beschäftigte bereits die Aufsicht. Sowohl die Post als auch Bertelsmann betonten, dass sie davon ausgehen, dass ein berechtigtes Interesse für den Adresshandel ausreichend sei.

Vor der direkten Anwendbarkeit der DSGVO 2018 durften Adressen von Verbrauchern recht einfach gehandelt werden. Ein Unternehmen, das die Privatadresse eines Verbrauchers hatte, konnte diese ungehindert weiterverkaufen, wenn der Käufer sie für Werbebriefe nutzen wollte. Diese wenig geliebten Schreiben enthalten z.B. Preisausschreiben und Verlosungen, um an weitere Anschriften von Kunden und werberelevante Informationen über sie zu kommen.

Der Präsident des Deutschen Dialogmarketingverbands (DDV), Patrick Tapp, warnte angesichts des drohenden Verbots vor schwerwiegenden wirtschaftlichen Folgen, denn „selektierte Briefwerbung" sei „ein wichtiger Motor für die europäische Volkswirtschaft". So könne ein regionaler Anbieter von Wärmepumpen mithilfe des Adresshandels Menschen ansprechen, die in Häusern wohnen, für die seine Produkte geeignet seien. Der DDV schätzt, dass es allein in Deutschland mehr als 1.000 Adresshändler gibt. Die laut gewordenen Ansichten deutscher Landesdatenschützer seien nichts weiter als eine von vielen Rechtsmeinungen, weitergehende Änderungen könnten nur auf EU-Ebene erfolgen. Der DDV geht davon aus, dass Direktmarketer neben den Adressen weitere Merkmale speichern dürfen wie Alter, Beruf oder Angaben zur gemieteten oder gekauften Wohnung. Gerade für junge Unternehmen sei es für die Kundenakquise wichtig passgenau Werbung per Post zu verschicken. Dies setzt laut Brink aber voraus, „dass die Werbeindustrie die Wünsche und die Vorlieben des Verbrauchers auch kennt, also zuvor sogenannte Profile mit Interessen und bisherigem Kaufverhalten anlegt. Niemand muss sich zu Werbezwecken vorab durchleuchten lassen."

Unterstützung bekommen die Datenschützer vom Verbraucherzentrale Bundesverband (vzbv). Florian Glatzner, Referent im Team Digitales und Medien, meinte: „Verbraucher gehen nicht davon aus, dass ein Unternehmen ungefragt ihre Daten an andere, völlig fremde Unternehmen verkauft und sie von diesen anderen Unternehmen dann plötzlich unerwünscht Werbung bekommen."

Eine lange umkämpfte Reform des Bundesmeldegesetzes von 2013 sieht bereits vor, dass zumindest Einwohnermeldeämter persönliche Daten der Bürger nur dann an Firmen für Werbung und Adresshandel weitergeben dürfen, wenn die Betroffenen ausdrücklich eingewilligt haben. Die Bürger können generell gegenüber der Meldebehörde oder gesondert gegenüber Unternehmen zustimmen. Die Ämter sollen in Stichproben oder anlassbezogen prüfen, ob eine Einwilligungserklärung vorliegt (Wischmeyer, Bitte keine Werbung, SZ 04.05.2022; Krempl, Direktmarketing: Datenschützer planen weitgehendes Adresshandelsverbot, www.heise.de 05.05.2022, Kurzlink: https://heise.de/-7075325).

Bundesweit

vzbv verklagt Tesla wegen Wächtermodus

Der Verbraucherzentrale Bundesverband (vzbv) hat gegen den US-amerikanischen Elektroautohersteller Tesla vor dem Berliner Landgericht Klage erhoben, weil das Unternehmen gegenüber seiner Kundschaft verschweigt, dass es gegen die Datenschutz-Grundverordnung (DSGVO) verstößt, wenn es in seinen Autos den Wächtermodus nutzt. Außerdem soll Tesla mit Werbeaussagen zur CO_2-Ersparnis in die Irre führen. In dem seit 2019 von Tesla angebotenen „Wächtermodus" oder „Sentry Mode" zeichnet das geparkte Auto Videos von der Umgebung auf, wenn es eine auffällige Bewegung feststellt. Wechselt ein Tesla-Auto derart in den „Alarm"-Zustand, erhalten die Besitzer eine Warnung auf ihrer Tesla-App.

Dabei müssten sich die Tesla-Nutzenden von den Menschen, die zufälligerweise erfasst werden, einwilligen lassen, dass deren personenbezogenen Daten verarbeitet werden dürfen, meint Heiko Dünkel, der im vzbv das Team Rechtsdurchsetzung leitet: „Wer die Funktion nutzt, verstößt daher gegen das Datenschutzrecht und riskiert ein Bußgeld." Im Grunde könne der Wächtermodus im öffentlichen Raum überhaupt nicht rechtskonform genutzt werden, da die Fahrzeugumgebung anlasslos aufgezeichnet wird.

Der vzbv kritisiert, dass dennoch der Wächtermodus für deutsche Straßen zugelassen sei. Um Lücken im Zulassungsverfahren zu schließen, müssten der Bundesdatenschutzbeauftragte und das Kraftfahrt-Bundesamt stärker zusammenarbeiten. Geprüft werden müsse,

so Marion Jungbluth, die im vzbv das Team Mobilität und Reisen leitet, ob eine Pflicht zur Datenschutz-Folgenabschätzung eingeführt werden sollte.

Der vzbv hatte Tesla im Dezember 2021 abgemahnt und eine Teil-Unterlassungserklärung zu mehreren Klauseln in der Datenschutzerklärung des Unternehmens erhalten. Der Wächtermodus blieb offenbar dabei aus Sicht der Verbraucherschützer zu wenig berücksichtigt.

Zudem beanstandet der vzbv Teslas Werbeaussage, das Elektroauto Model 3 stoße „0 g/km“ CO_2 aus, sowie das „Tesla-Credo“: „Je schneller wir unsere Abhängigkeit von fossilen Brennstoffen überwinden und eine emissionsfreie Zukunft verwirklichen, desto besser.“ Damit wird, so der vzbv, Teslas Emissionshandel ausgeblendet. Das Unternehmen habe allein im Jahr 2020 rund 1,6 Milliarden US-Dollar durch den Verkauf von „Emission Credits“ eingenommen, womit andere Hersteller die Grenzwerte ihrer Fahrzeugflotten überschreiten könnten. Über den Verkauf der Emissionsrechte informiere das Unternehmen, so der vzbv, vor einer Bestellung eines Fahrzeugs nur auf Seite 30 des auf Englisch verfassten Umweltverträglichkeitsberichts, der auf der Website heruntergeladen werden konnte.

Zum Wächtermodus hatte bereits das Netzwerk Datenschutzexpertise im Oktober 2020 befunden, dass deshalb Tesla-Autos in Europa eigentlich nicht zugelassen werden dürften. Tesla hatte hierfür im selben Jahr den BigBrotherAward in der Kategorie Mobilität erhalten. In diesem Jahr versandte der Sicherheitschef der Berliner Polizei ein Schreiben an die Dienststellen, laut dem Aufnahmen durch den Wächtermodus in Tesla-Autos auf Liegenschaften der Polizei nicht zulässig sein sollen (vgl. in diesem Heft S. 185 sowie DANA 4/2020, 227 ff.; Wilkens, Verbraucherschützer verklagen Tesla wegen Wächtermodus und Werbung, www.heise.de 19.07.2022, Kurzlink: https://heise.de/-7183240).

Bundesweit

Digitalcourage klagt gegen DB Navigator

Ohne die Smartphone-App „DB Navigator“ ist erfolgreiches Zugfahren in Deutschland kaum noch möglich. Sie bietet Information über Verspätungen und Anschlusszüge, Ticketkauf an Bord und mehr. Einige Services sind auf anderem Wege gar nicht mehr zu bekommen. Die App forscht zugleich die Nutzenden aus. Der IT-Sicherheitsforscher Mike Kuketz hat den DB Navigator gründlich analysiert und dabei erhebliche Datenschutzprobleme festgestellt. Wenn die App genutzt wird, fließen im Hintergrund Informationen an Adobe, Google und Co. Die DB-App lässt es nicht zu diese abzuschalten. Der auf IT- und Datenschutzrecht spezialisierte Anwalt Peter Hense hält die App deshalb für rechtswidrig. Der Datenschutzverein Digitalcourage e.V. hat gemeinsam mit den Vorgenannten die Bahn Ende April 2022 dazu aufgefordert die Mängel innerhalb von zwei Monaten zu entfernen. Doch die Bahn signalisierte, dass sie das Tracking nicht beenden will. Deshalb kündigte Digitalcourage eine gerichtliche Klage an.

Die Deutsche Bahn (DB) wehrt sich gegen die Vorwürfe. Die Kritik an der Reiseauskunfts- und Buchungsanwendung sei „haltlos“. Bei der App-Nutzung flößen „keinerlei Kundendaten an Drittanbieter“. Alle Dienstleister, mit denen man bei der App zusammenarbeite, so die DB, „sind vertraglich gebunden, handeln nicht in eigenem Interesse und streng nach Weisung der DB“. Es handle sich so nicht um Dritte im Sinne der Datenschutz-Grundverordnung (DSGVO): „Alle Technologieanbieter, die im DB Navigator in der Kategorie ‚erforderlich‘ aufgelistet sind, verarbeiten Daten ausschließlich zu den Zwecken die vielfältigen Funktionen und die Stabilität der App für mehr als zwei Millionen Kunden täglich zu gewährleisten.“ Dabei seien „keine identifizierenden personenbezogenen Informationen“ im Spiel, sondern nur pseudonymisierte. Diese stellten sich „für den einzelnen Anbieter isoliert“ sogar als „anonyme Dateninhalte“ dar.

Keiner der US-Partner wie Adobe, Google oder Optimizely sei in der Lage „die Daten an anderer Stelle oder gar zu eigenen Marketingzwecken einzusetzen“. Ein Webseiten- oder App-übergreifendes Nachverfolgen von Kunden mit den umstrittenen Cookies sei nicht möglich. Der Konzern lege generell „großen Wert auf die sparsame Erhebung und den sorgsamen Umgang“ mit Kundendaten. Man habe zu den Bedenken von Digitalcourage detailliert Stellung genommen und ein Gespräch angeboten, heißt es weiter. Darauf habe der Verein aber nicht reagiert. Eine Sprecherin hob hervor: „Wir nehmen die jüngsten öffentlichkeitswirksamen Aktivitäten daher mit Befremden zur Kenntnis.“ Konzernexperten stünden ferner in engem Austausch mit den zuständigen Datenschutzbehörden.

Mike Kuketz, der im Rahmen einer technischen Analyse der Navigator-App die Tracker ausfindig gemacht hatte, zeigte sich dagegen erstaunt, „dass es große Konzerne wie die DB nicht schaffen dem Thema Datenschutz mit der gebotenen Ernsthaftigkeit zu begegnen“. Dabei seien bei diesen die Ressourcen dafür vorhanden. Der Verweis auf die Definition von „Dritten“ in der DSGVO lenke die Diskussion nur um auf einen gar nicht beanstandeten Sachverhalt. Der Experte bietet in einem Blogeintrag Tipps, wie sich das „Datensendeverhalten“ zumindest von Android-Apps beeinflussen und unerwünschtes Tracking so verhindern lässt. Er verwies auch auf eine Analyse der „Stiftung Warentest“, wonach es die Bahn-App mit dem Datenschutz „nicht so genau“ nimmt. Darüber erfolgende Transfers persönlicher Informationen seien „kritisch“ einzustufen (Digitalcourage e.V., DB-Schnüffel-Navigator Wir klagen gegen die Bahn, E-Mail v. 20.07.2022; Krempl, Deutsche Bahn: Kritik von Datenschützern am DB Navigator ist „haltlos“, www.heise.de 23.07.2022, Kurzlink: https://heise.de/-7188327).

Bundesweit

Schufa bewegt sich – langsam

Die Schufa – die Schutzgemeinschaft für allgemeine Kreditsicherung – hat ein Image-Problem, weil sie ein Datenschutzproblem hat. Dies beruht u.a. darauf, dass sie bisher äußerst intransparent agiert. Sie beeinflusst mit ihren Kreditbewertungen den Alltag von vielen Menschen in Deutschland, legt aber z.B. nicht die Formeln zur Berechnung

der „Schufa-Scores" offen, die darüber entscheiden, ob und wie Menschen im Wirtschaftsleben unterwegs sein können. Die Auskunftei ist keine öffentliche Stelle, wie viele meinen. Sie ist eine Aktiengesellschaft mit verschiedenen Anteilseignern, darunter Sparkassen und Genossenschaftsbanken, Kredit- und Privatinstitute sowie Händler. Mehr als eine Milliarde Informationen hat die Schufa nach eigenen Angaben gespeichert, zu rund 68 Millionen Menschen in Deutschland. Daraus berechnet das Unternehmen die berüchtigten Scores, die Vertragspartnern wie Banken und Händlern Aufschluss über die Bonität ihrer Kunden geben sollen. Wie wahrscheinlich ist es, dass ein Kunde seinen Kredit abbezahlt? Drohen Ausfälle beim Ratenkauf?

• Mehr Transparenz

Von dem schlechten Image will sich die Schufa lösen und hat erste Schritte einer angekündigten Transparenzoffensive umgesetzt: Der Auftritt im Netz wurde rundum erneuert; neue Tools sollen Verbrauchern das Zustandekommen ihrer Scores besser erklären. Daneben gibt es einen Video-Chatbot, der sämtliche Fragen beantworten will. Die Möglichkeit, seine Daten kostenlos einzusehen, hebt die Schufa neuerdings besser hervor.

Die Auskunftei listet nun auf, welche Faktoren die Bonitäts-Punktzahl beeinflussen. Dazu zählen die Zahl der Girokonten und Kreditkarten, Konten bei Versandhändlern und Leasingverträge, nicht jedoch Handyverträge. Sie gibt Tipps auf der Seite, wie Verbraucher ihren Score verbessern können, wenngleich dies noch wenig konkret ist. So rät die Schufa etwa zu überprüfen, welche Girokonten und Kreditkarten überflüssig sind. Deren Kündigung könne den Score langfristig erhöhen. Übersehene Rechnungen und Ratenzahlungen sollten schnellstmöglich beglichen werden.

In der Vergangenheit hatte die Auskunftei stets argumentiert, dass Details zur Score-Berechnung ihre Geschäftsgeheimnisse offenlegen würden. Daneben erklärte sie, sie wolle verhindern, dass Nutzer ihr finanzielles Verhalten speziell für einen guten Score anpassen. Verbraucherschützer haben die Argumente aber nie überzeugt. So meint Gert Wagner vom Sachverständigenrat für Verbraucherfragen: „Ist das Verhalten ursächlich für die Kreditwürdigkeit, dann ist eine Verhaltensänderung ja keine Manipulation, sondern erwünscht." Heute ist von Geschäftsgeheimnissen und Score-Manipulation zumindest offiziell keine Rede mehr. Eine Transparenz der genauen Scoreberechnung wird weiterhin nicht gewährt.

An die gemäß der Datenschutz-Grundverordnung (DSGVO) kostenlose Datenkopie kommen Nutzer jetzt leichter. Die Option findet sich direkt auf der Startseite. Bisher verdiente die Schufa mit kostenpflichtigen Auskünften viel Geld, weshalb sie die Betroffenen bislang lieber in ihre kostenpflichtigen Angebote, darunter die klassische Schufa-Auskunft oder ein Online-Abonnement mit Live-Scores, lockte. Dass Nutzer einen kostenfreien Datenabzug bestellen können, hatte die Auskunftei hingegen hinter zahlreichen Klicks verborgen. Die Schufa erklärte: „Die Kritik, die kostenlose Datenkopie ‚zu verstecken', haben wir aufgenommen."

Zudem hat sich die Auskunftei vorgenommen in einfacher Sprache zu kommunizieren, so Schufa-Vorstandschefin Tanja Birkholz: „Wir wollen weg von der unnahbaren Instanz, hin zu einem Dialog auf Augenhöhe." Den Anfang soll ein Video-Chatbot machen. Nutzer können eine beliebige Frage stellen und bekommen ein Video ausgespielt, in dem Mitarbeiter die passenden Antworten liefern sollen. Der Video-Chatbot befindet sich allerdings noch in der Lernphase. Mit zunehmender Nutzung sollen die Antworten treffsicherer werden.

• Ökonomische Hintergründe

Ganz freiwillig sind die Bemühungen nicht. Die Transparenzoffensive ist nötig geworden, nachdem sich die Auskunftei zunehmendem Druck ausgesetzt sieht. Es gibt harsche Kritik von Daten- und Verbraucherschützern am umstrittenen Projekt „CheckNow", womit die Schufa in bestimmten Fällen die Verbraucher auch anhand ihrer Kontoauszüge bewerten wollte, was letztlich aufgegeben wurde (DANA 1/2021, 40 ff.). Ein Bieterwettstreit um die Schufa heizte den Reformwillen an (DANA 4/2021, 240 ff). Der schwedische Investmentfonds EQT verfolgte das Ziel bis zu 100% der Anteile am Unternehmen zu kaufen. Ursprünglich hatten die Schweden mit der französischen Großbank Société Générale vereinbart deren Anteil von knapp 10% zu übernehmen. Die genossenschaftliche Teambank wollte den Einstieg verhindern und ihre bestehende Minderheitsbeteiligung aufstocken. Sie gehört zur DZ-Bank-Gruppe, bei der die Anteile der Volks- und Raiffeisenbanken an der Schufa gebündelt sind. Sie haben als Bestandsaktionäre ein Vorkaufsrecht für die Anteile. Das Bundeskartellamt hatte beide Vorhaben bereits freigegeben. Die neuen Kaufinteressenten und der Schufa-Vorstand überboten sich im Rahmen des Bieterstreits mit Versprechungen zur Datenschutz- und Verbraucherfreundlichkeit. Vor allem EQT gab sich als Reformer. Mit Strategiepapieren, an denen auch Verbraucherorganisationen mitgewirkt haben sollen, machte der Investor großzügige Ankündigungen: Verbraucher sollen etwa kostenlos Daten und Löschfristen in einer Handy-App einsehen können. Anfang Juli 2022 kam dann die Nachricht, dass der Übernahmeplan von EQT gescheitert ist. Die Genossenschaftsbanken haben ihr Vorkaufsrecht ausgeübt und damit ihren Schufa-Anteil auf 27,2% ausgebaut. Bei den Sparkassen liegen 26,4%; sie wollen weiter aufstocken. Ob dies nun den Reformeifer bremst, muss sich zeigen.

Nicht zuletzt greifen auch Gerichte und Behörden immer wieder in das Geschäftsmodell der Wirtschaftsauskunfteien ein (DANA 2/2021, 142). Im September 2021 stellte z.B. die Datenschutzkonferenz, der Zusammenschluss der Aufsichtsbehörden aus Bund und Ländern, klar, dass Handyvertragsdaten ohne Einwilligung nicht gespeichert werden dürfen (DANA 1/2022, 34).

• Kommentar des Verbraucherschutzes

Mathias Hufländer, Rechtsexperte bei der Verbraucherzentrale Bremen, sieht in den jüngsten Bemühungen einen Schritt in die richtige Richtung, insbesondere bei der kostenlosen Datenkopie: „Wir hatten diesbezüglich häufiger Anfragen von Verbrauchern, die nur das kostenpflichtige Angebot gefunden haben. Dies dürfte sich damit erledigen."

Die Erklärungen zum Scoring gehen ihm noch nicht weit genug: „Die Verbraucher müssen erfahren, welche Faktoren ihr Scoring konkret und in welcher Form beeinflussen." Es brauche zudem klare gesetzliche Regelungen, welche Informationen beim Scoring berücksichtigt werden dürfen. Man dürfe sich nicht allein auf die freiwilligen Bemühungen der Auskunftei verlassen.

Von der Schufa heißt es wiederum: „Weitere Schritte zu mehr Transparenz sind in Planung." Das Herzstück der Transparenzoffensive lässt noch auf sich warten. Die Schufa will einen Score-Simulator bereitstellen. Nach bisherigen Planungen soll dieser zunächst verschiedene Merkmale abfragen. Etwa: Wann wurde das erste Bankkonto eröffnet? Oder: Wie viele Kreditkarten besitzt der Nutzer? Anschließend berechnet der Simulator den ungefähren Schufa-Score des Nutzers und zeigt ihm zusätzlich, wo er im Vergleich zu den anderen Bundesbürgern steht. Der Simulator soll Verbrauchern zudem erklären, wie sich der Score im Laufe der Zeit verändern wird. Konkret bedeutet das: Nach wie vielen Monaten ist der Score wieder auf dem Ursprungsniveau, wenn ein Verbraucher etwa ein zusätzliches Girokonto eröffnet (Meyer, Die Schufa lüftet ihr Geheimnis, Die Welt, 21.04.2022, 10; Banken kontrollieren Schufa, SZ 01.07.2022, 21).

Baden-Württemberg

Untersuchungsausschuss wegen Strobls Durchstecherei an Journalisten

Der Landtag von Baden-Württemberg hat einen Untersuchungsausschuss zur Klärung der Affäre um die Weitergabe vertraulicher Informationen durch Innenminister Thomas Strobl (CDU) eingesetzt. Sowohl Regierung als auch Opposition stimmten dafür. Der Ausschuss soll auch Hintergründe zum Vorwurf des sexuellen Missbrauchs gegen den Inspekteur der Polizei, ranghöchster Polizist des Landes, in diesem Zusammenhang aufklären.

Der SPD-Abgeordnete Sascha Binder begründete den Antrag der Oppositionsfraktionen SPD und FDP: „Polizeibeamte haben ein Recht darauf, dass sich auch ihre Führung an Recht und Gesetz hält". Die Frage sei, ob es schon Machtmissbrauch gewesen sein könnte den von Strobl favorisierten Beamten zum Polizeiinspekteur zu machen. Strobl soll sich im Vorfeld für den dann beschuldigten Mann starkgemacht haben. FDP-Fraktionschef Hans-Ulrich Rülke: „Der Innenminister hat offenbar einiges zu verbergen. Das schreit nach einem Untersuchungsausschuss." Auch die Regierungsfraktionen stimmten dem Ausschuss überraschend zu, was der Grünen-Abgeordnete Oliver Hildenbrand begründete: „Aufklärung im Fall des sexuellen Missbrauchs ist notwendig." Sie betreffe die ganze Gesellschaft. Strobls Verhalten sei ein „Kommunikationsfehler"; der Opposition warf er „haltlose, völlig überzogene Vorwürfe" vor.

Strobl, der auch Chef der Landes-CDU ist, steht unter Druck, weil er ein Anwaltsschreiben in dem Verfahren an einen Journalisten weitergeben hatte, um „maximale Transparenz" zu schaffen, so später seine Begründung. Es habe sich um „ein vergiftetes Gesprächsangebot" gehandelt. Später verweigerte er die Ermächtigung der Staatsanwaltschaft zur Ermittlung gegen ihn in dieser Sache. Strobl steht im Verdacht den Reporter angestiftet zu haben verbotenerweise „Mitteilungen über Gerichtsverhandlungen" gemacht zu haben. Der Untersuchungsausschuss soll nun das Agieren Strobls und seines Ministeriums beleuchten.

Beide Seiten haben Gutachten vorgelegt. Die SPD gab eine Analyse beim Landesbeauftragten für den Datenschutz, Stefan Brink, in Auftrag, die feststellte, dass die Weitergabe des Schreibens das Datenschutzrecht verletze und deshalb „rechtswidrig" war. Strobl präsentierte ein Gutachten des Medienanwalts Christian Scherz, wonach Strobl im Rahmen seiner Kompetenzen gehandelt habe. Der fragliche Brief des Anwalts sei kein amtliches Dokument und dessen Weitergabe deshalb nicht strafbar.

Aus Reihen der Grünen wird häufig an den Fall Wolfgang Schmidt erinnert, den aktuellen Kanzleramtsminister in Berlin. Der Sozialdemokrat hatte, als während des Bundestagswahlkampfs 2021 die Staatsanwaltschaft das Ministerium des damaligen Bundesfinanzministers Olaf Scholz durchsuchte, Teile des Gerichtsbeschlusses bei Twitter ins Netz gestellt. Auch damals ging es um eine „verbotene Mitteilung über Gerichtsverhandlungen". Am Ende zahlte Schmidt 5.000 € an zwei gemeinnützige Einrichtungen und der Fall war erledigt.

Hintergrund sind Vorwürfe gegen den Landespolizeiinspekteur. Der 47-jährige Mann soll einer Kriminalkommissarin, die in den höheren Dienst wechseln wollte, in einer Videobesprechung die Beförderung gegen Sex angeboten haben. Die Ermittlungen zu dem Fall laufen seit Dezember 2021. Der Beamte wurde vom Amt suspendiert (Landtag setzt Untersuchungsausschuss zu Strobl-Affäre ein, www.zeit.de 01.06.2022, Ferstl, Landtag untersucht die Affäre Strobl, SZ 02.06.2022, 5).

Baden-Württemberg

Brink will hinschmeißen

Das Land Baden-Württemberg wird voraussichtlich einen neuen Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI) suchen müssen. Der aktuelle Stelleninhaber, Stefan Brink, kündigte seinen Mitarbeitern am 13.07.2022 in einer internen Versammlung der Behörde an, dass er Ende 2022 aus dem Amt scheiden und nicht wieder kandidieren werde. Der LfDI wird laut Gesetz auf Vorschlag der Landesregierung vom Landtag gewählt. In der Mitarbeiterversammlung soll Brink gesagt haben, es gebe „kein Zerwürfnis" mit Grün-Schwarz. Er habe sich aber mit der Landesregierung nicht auf künftige Projekte einigen können. Regierungssprecher Arne Braun bestätigte die Personalie auf Anfrage, äußerte sich aber zunächst nicht zu den Hintergründen.

Es wird spekuliert, dass in den Verhandlungen Meinungsunterschiede über die weitere Landesstrategie zur Digitalisierung auftraten. Auch das im Koalitionsvertrag von Grünen und CDU angekündigte „Transparenzgesetz", das aus dem Landes-Informationsfreiheitsgesetz entwickelt werden soll, könnte Konfliktstoff geboten haben. Es ist bekannt, dass Brink hier eine weitgehende Lösung anstrebt.

Ministerpräsident Winfried Kretschmann (Grüne) erweckt immer wieder

den Eindruck, er sehe hiesige Datenschutz-Standards als überzogen und hinderlich an. Die Corona-Warn-App, klagte er z.B. 2021, sei wegen des Datenschutzes „nur eine Krücke“.

Der promovierte Jurist Brink war Anfang 2017 aus Rheinland-Pfalz nach Stuttgart gewechselt (DANA 1/2017, 48 f.). Er erwarb sich den Ruf eines oft unbequemen Kritikers der Landespolitik. So griff er beispielsweise in Pläne des Kultusministeriums für eine digitale Bildungsplattform mit Software des US-Herstellers Microsoft ein und setzte so durch, dass die Pläne geändert wurden (DANA 3/2021, 180). Auch eine öffentlich ausgetragene Kontroverse mit dem Tübinger Oberbürgermeister Boris Palmer oder ein hohes Bußgeld für den Fußballverein VfB Stuttgart gingen durch die Medien (DANA2/2021, 114 f.). Zuletzt erzeugte ein Gutachten Brinks für Aufsehen, in dem er dem Innenminister, Vize-Regierungschef und CDU-Landesvorsitzenden Thomas Strobl vorwirft mit einer Indiskretion rechtswidrig gehandelt zu haben (s.o.). Die Staatsanwaltschaft Stuttgart ermittelt in der Angelegenheit.

Für seine abgelaufene Amtszeit zog Brink eine positive Bilanz: „Das waren sechs großartige Jahre in Baden-Württemberg, wir haben eine Menge aufgebaut, das Bild und Ansehen des Datenschutzes weiterentwickelt.“ Unter seiner Leitung ist die Dienststelle des Datenschutzbeauftragten zu einer Behörde mit mehr als 70 Planstellen ausgebaut worden. Jetzt sucht der 56-jährige Jurist nach eigenen Worten eine neue Herausforderung. Er werde dem Thema aber treu bleiben und ab dem kommenden Jahr von Berlin aus in einer privaten Tätigkeit das „Megathema Digitalisierung“ betreuen.

Aus der SPD-Landtagsfraktion heißt es, die Landesregierung wolle einen unliebsamen Kritiker loswerden. Die Sozialdemokraten sowie die FDP-Fraktion bedauerten Brinks Weggang und betonten seine Dienste für den Datenschutz (Habermehl, Baden-Württembergs Datenschutzbeauftragter Brink hört auf, www.badische-zeitung.de 13.07.2022; Landes-Datenschutzbeauftragter Stefan Brink will seinen Vertrag nicht verlängern, www.swr.de 13.07.2022).

Bayern

Keine Sanktion wegen großer Buchbinder-Datenpanne

Teils höchst persönliche Daten von drei Millionen Kundinnen und Kunden des Autovermieters Buchbinder, insgesamt zehn Terabyte, standen Anfang 2020 wochenlang völlig ungeschützt zum Abruf bereit. Es ging um Informationen wie Adressen, Telefonnummern, Kontoverbindungen, aber auch detaillierte Unfallberichte. Die Ursache des Lecks lag in einem eher profanen Konfigurationsfehler eines externen Backup-Servers: Über den offenen Port 445 hatten offensichtlich fahrlässig agierende Admins SMB-Zugriff gestattet und damit die Archive aus dem Internet einsehbar gemacht. Sämtliche Daten waren unverschlüsselt zu finden, ein Passwort für den Zugang war nicht erforderlich.

Die nicht vorhandene Zugriffssicherung stellt einen erheblichen Verstoß gegen die DSGVO dar. Als zuständige Aufsichtsbehörde für die Buchbinder-Gruppe hatte sich das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) mit Sitz in Ansbach der Sache angenommen. Für Erstaunen hatte die Behörde bereits früh mit der Einschätzung gesorgt, dass es sich bei der Datenpanne nicht um einen Fall nach Artikel 34 der DSGVO handelt, wonach der Autovermieter alle betroffenen Kunden über die Datenpanne hätte informieren müssen, sofern dadurch „voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten“ der Betroffenen entstanden wäre. Auf eine persönliche Unterrichtung zum mehr als schludrigen Umgang mit ihren Daten warten die Kunden, die über die Medien von der Panne erfuhren, bis heute.

Datenschutzexperten gingen davon aus, dass die Behörde ein hohes Bußgeld verhängen würde, zumal hier ein eindeutiger Verstoß unter anderem gegen Artikel 32 DSGVO vorlag, der die technischen Anforderungen zum Schutz von Daten definiert. Im April 2022 teilte die Behörde auf Anfrage von Journalisten mit, dass sie die Akte bereits im Dezember 2021 geschlossen habe. Es habe kein Anlass bestanden „von Abhilfe- beziehungsweise Sanktionsbefugnissen Gebrauch zu machen“. Maßgebliche Umstände seien dabei insbesondere „die Zurechenbarkeit des der Datenschutzverletzung zugrunde liegenden Fehlverhaltens und umfassende und effektive eigenverantwortliche Abhilfemaßnahmen sowie die pandemiebedingt angestiegene Sanktionsempfindlichkeit des Unternehmens“ gewesen. Im Ergebnis kommt der Autovermieter für seine Datenpanne also ohne jegliche Sanktion durch die Behörde davon.

Der Sachverhalt begründet, so offenbar die Ansicht des BayLDA, grundsätzlich keine Verletzung von Artikel 32 der DSGVO. Die Behörde meint, es gehöre zu den Aufgaben des Verantwortlichen selbst – also der Buchbinder-Gruppe – zu überprüfen, ob Abrufe erfolgt sind, beispielsweise „durch die Auswertung von Log-Dateien samt übertragenen Datenmengen“. Die Annahme des BayLDA einer „geringen Eintrittswahrscheinlichkeit“ des Vertraulichkeitsverlustes ist erstaunlich, zumal der Zugriff eines c't-Redakteurs auf die Buchbinder-Kundendaten beispielsweise von der ARD-Tagesschau dokumentiert wurde.

Könne der Betreiber des offenen Servers, so das BayLDA, nachweisen, dass es nur eine „begrenzte, gegebenenfalls sogar individuell identifizierbare und damit spezifisch zu bewertende Anzahl von Akteuren“ gab, die Zugriff auf die Daten gehabt hatten, so sei das zu berücksichtigen. Durch Analysen des Netzwerkverkehrs habe Buchbinder „eine geringe Eintrittswahrscheinlichkeit eines Abrufs mit dem Zweck eines Datenmissbrauchs“ ermittelt. Sowohl Redakteure der c't wie auch der Zeit sowie der Tippgeber hatten mehrfach auf die Daten zugriffen, weshalb eine ganze Menge unterschiedlicher IP-Adressen in den Log-Dateien hätten aufgetaucht sein müssen. Überdies könnten bei einem Angriff von Unbekannt die Log-Dateien nachträglich manipuliert worden sein.

Fabian Schmieder, Professor für Medienrecht und Datenschutz an der Hochschule Hannover, kritisierte u.a. die Annahme der Behörde, dass es auf die Intention der Personen ankommen soll, die auf die Daten zugegriffen haben. Maßgeblich sei allein, dass durch die Fehlkonfiguration ein unberechtig-

ter Zugriff faktisch ermöglicht wurde. Nach seiner Ansicht liegt ein schwerwiegender Verstoß gegen Artikel 32 Absatz 1 DSGVO vor, der ein hohes Bußgeld nahelegt (Heidrich, Kein Bußgeld für die Datenpanne bei Buchbinder, www.heise.de 06.05.2022, Kurzlink: https://heise.de/-7072949).

Berlin

Sicherheitschef der Polizei warnt vor Teslas Wächtermodus

Der Sicherheitschef des Berliner Polizeipräsidiums und Landeskriminalamts hat mit einem Rundschreiben vom 22.06.2022 vorgegeben, dass Elektroautos von Tesla wegen der in ihnen eingebauten Videokameras nur eingeschränkt auf Liegenschaften der Berliner Polizei gelangen dürfen, weil die Elektroautos Mitarbeitende, Dritte und die Liegenschaften selbst und den Datenschutz gefährden. Die Autofahrer selbst erfahren nicht, wie die Daten dann weiterverarbeitet werden. Thilo Cablitz, Pressesprecher der Berliner Polizei, erläuterte, dass noch kein generelles Einfahrverbot bestehe. Die Regelungslage werde noch abschließend je nach Liegenschaft abgestimmt. Auch werde die fortwährende Entwicklung der IT in Kraftfahrzeugen berücksichtigt. Dem Schreiben des Sicherheitschefs wird zunächst keine Verbotswirkung zugemessen; es diene der Sensibilisierung.

Schon bisher dürfen gemäß Cablitz in sämtlichen Sicherheitsbereichen der Polizei Berlin keine Ton-, Foto- und Filmaufnahmen angefertigt werden, wenn sie nicht dienstlich erforderlich und dazu geeignet sind sicherheitsrelevante Interessen zu verletzen. Wie bisher gelte, jede und jeder sei erst einmal selbst verantwortlich dafür Sorge zu tragen, dass keine entsprechenden Aufnahmen gefertigt werden, ob nun mit dem Smartphone, der Kamera oder durch die das Umfeld überwachenden Automobil-IT.

Der Berliner Polizei sei deutlich geworden, dass Tesla-Autos mit den Kameras ständig und ereignisunabhängig bewegte Bilder der Fahrzeugumgebung aufzeichnen, diese Aufnahmen in die Niederlande ausleiten und dort auf Tesla-Servern dauerhaft gespeichert würden. Im seit 2019 von Tesla angebotenen Wächtermodus (Sentry Mode) zeichnet das Auto Videos von der Umgebung auf, wenn es eine auffällige Bewegung feststellt. Wenn ein Tesla-Auto derart in den „Alarm"-Zustand wechselt, erhalten die Besitzer eine Warnung auf ihrer Tesla-App.

Dafür genügt es, dass eine Person oder ein anderes Fahrzeug nahe am Auto vorbeikommen. Deshalb und aus weiteren Gründen äußerte 2020 der frühere schleswig-holsteinische Datenschutzbeauftragte Thilo Weichert vom Netzwerk Datenschutzexpertise starke Bedenken wegen Teslas Datenschutzverträglichkeit in Europa und verlieh einen BigBrother-Award (DANA 4/2020, 227 ff.).

Heikel sind dauerhaft aktivierte Videoaufzeichnungen für die Berliner Polizei auch, weil mit ihnen Sicherheitsbereiche wie Munitionsbunker, Zivilwagen mit Tarnkennzeichen und Bereiche von Zivilermittlern oder Spezialkräften von den Tesla-Kameras erfasst werden könnten. Der Berliner Sicherheitschef hat vorgegeben, dass seine Tesla-Warnung „als behördenweite Maßnahme von allen Verantwortlichen für ihre jeweiligen polizeilichen Liegenschaften gleichermaßen umzusetzen ist".

Persönlich betroffen von der „Anordnung" ist u.a. Thomas Goldack, Leiter der Direktion 2 im Westen der Stadt. Er fährt einen Tesla, der am Tag des Anschreibens auf seinem persönlichen Parkplatz auf dem Polizeigelände, markiert von einem blauen Parkschild mit der Aufschrift „L Dir 2", gesehen wurde. Die Gewerkschaften und Berufsverbände reagierten unterschiedlich. Benjamin Jendro, Sprecher der Gewerkschaft der Polizei (GdP), zeigte sich problembewusst: „Die heutigen technischen Möglichkeiten sind sehr weitreichend und machen es notwendig Sicherheitsmaßnahmen auf Liegenschaften stets zu optimieren. Klar ist aber auch, dass vieles noch immer auf den Menschen selbst ankommt, der die Technik nutzt."

Dagegen bezeichnete Jörn Badendick vom Verband „Unabhängige in der Polizei" den Vorgang als grotesk: „Wenn Mitarbeiter des höheren Dienstes aus Bequemlichkeit mit ihren Privatfahrzeugen für die Polizei Berlin zum Sicherheitsrisiko werden, erwarte ich von den unabhängigen Datenschutzbeauftragten die sofortige Aufnahme von Ermittlungen. Das Ganze ist ein Vorgehen à la Pippi Langstrumpf – ich mache mir die Welt, wie sie mir gefällt. Richtigerweise müsste erst geprüft werden und dann die Erlaubnis zum Befahren des Geländes erteilt werden."

Unter anderen Umständen profitiert die Polizei von Teslas Überwachungsmodus. Nach Unfällen können Ermittler mit richterlichem Durchsuchungsbeschluss sich in die europäische Datenzentrale von Tesla oder in den internen Speicher eines Autos einloggen.

Auch die Berliner Datenschutzbeauftragte (BlnBDI) befasste sich mit dem Wächtermodus und stellte fest, dass dieser nicht grundlos durchgehend auf Parkplätzen aktiviert sein und Bilder von der Umgebung nicht aufzeichnen darf. Wenn es Beschwerden wegen des aktivierten Modus gebe, werde die Aufsichtsbehörde ein Verfahren einleiten und den Fall prüfen, was zu einem Bußgeld führen könne. Teslas Sentry Mode hatte zuvor bereits die chinesische Regierung zu Bedenken geführt. Sie wolle Militärangehörigen und Mitarbeitern wichtiger Unternehmen die Nutzung von Tesla-Fahrzeugen verbieten. Die chinesische Regierung befürchtet, dass die von den E-Autos über Kameras und Sensoren gesammelten Daten durch den Datentransfer zu Tesla in die USA die nationale Sicherheit Chinas gefährden könnten (s.o. S. 180; Fröhlich, Berliner Polizei rudert zurück – vorerst doch kein Hausverbot für Teslas, www.tagesspiegel.de 23.06.2022; Wilkens, Wächtermodus: Tesla-Autos sollen nicht mehr auf Berliner Polizeigelände parken, www.heise.de 23.06.2022, Kurzlink: https://heise.de/-7151317).

Brandenburg

Kanzlerehepaar entsorgt sensible Daten im Hausmüll

Bundeskanzler Olaf Scholz und seine Ehefrau Britta Ernst, Bildungsministerin in Brandenburg, sind langjährige Politikprofis, praktizierten aber einen eher laxen Umgang mit wichtigen Dokumenten in ihrem Haushalt. Im Hausmüll fanden

sich wiederholt Dienstpapiere – darunter sogar Verschlusssachen, ohne dass diese vorher geschreddert oder anderweitig unkenntlich gemacht waren.

Gemäß Presseberichten waren auch vertrauliche Dokumente, die teils als „Verschlusssache – nur für den Dienstgebrauch“ eingestuft worden seien, im Restmüll zu finden. Nachbarn des Wohnkomplexes in der Potsdamer Innenstadt, den auch das SPD-Politikerpaar bewohnt, seien auf das Altpapier im Restmüll oder gar in transparenten Mülltüten vor dem Müllraum aufmerksam geworden. Die meisten der Papiere gingen dabei offenbar auf Britta Ernst zurück, die diese allenfalls ein- oder zweimal durchgerissen haben soll – und manchmal sogar gar nicht. Darunter befanden sich Auszüge aus dem Terminkalender der brandenburgischen Bildungsministerin, Einblicke in die Kleiderwahl der Kanzlergattin für wichtige Termine oder per E-Mail gestellte Anfragen für Englischkurse Ernsts.

Unter den wenig fachgerecht entsorgten Unterlagen befanden sich als vertraulich eingestufte Papiere, etwa kurz nach dem G7-Gipfel Ende Juni in Elmau ein Dokument, auf dem Kurzprofile der Partnerinnen und Partner der teilnehmenden Regierungschefs zu finden waren. Der „Organisationsstab Vorsitze“ im Auswärtigen Amt hatte der Kanzlergattin aufgeschrieben, wen sie als Gastgeberin des Partnerprogramms betreuen sollte. Unter dem Foto von Maria Serenella Cappello, der Ehefrau von Ministerpräsident Mario Draghi steht z.B. „Meidet die Öffentlichkeit“. Zur Frau von Japans Regierungschef Fumio Kshida heißt es: „Sekretärin bei Mazda“.

Für solche Dokumente gelten strenge Umgangsregeln. Amtsträger werden von den Sicherheitsbehörden darin unterwiesen, wie sie diese behandeln sollen. Zum Umgang mit Verschlusssachen ermächtigt wird nur, „wer eine Sicherheitsprüfung zur Feststellung der erforderlichen Zuverlässigkeit bestanden hat“. Verschlusssachen-Dokumente „nur für den Dienstgebrauch“ dürfen Dienstgebäude nur verlassen, wenn dies auch dienstlich notwendig ist. Zudem müssten die Papiere so entsorgt werden, „dass der Inhalt weder erkennbar ist noch erkennbar gemacht werden kann“, so die Verwaltungsvorschrift des Bundes zum „materiellen Geheimschutz“ (Schult, G7? Ab in die Tonne, Der Spiegel Nr. 30 v. 23.07.2022, 23; Bericht: Kanzler Scholz und Gattin Ernst entsorgen Geheimdokumente im Hausmüll, www.rnd.de 22.07.2022).

Niedersachsen

VW-Fahrzeug-Assistenzerprobung führt zu 1,1 Mio.-Euro-Bußgeld

Der Wolfsburger Autobauer Volkswagen (VW) muss eine Geldbuße in Höhe von 1,1 Mio. Euro zahlen, weil es der Konzern und ein eingesetzter Dienstleister bei dem VW-Erprobungsfahrzeug mit dem Datenschutz nicht so genau nahmen und Überwachungskameras ohne erforderliche Kennzeichnung verwendeten. Die niedersächsische Landesbeauftragte für Datenschutz (LfD) Barbara Thiel erkannte als zuständige Datenschutzaufsichtsbehörde letztlich mehrere Verstöße gegen die Datenschutz-Grundverordnung (DSGVO) und verhängte die nicht unerhebliche Strafe. Die österreichische Polizei kontrollierte das Testfahrzeug 2019 bei Salzburg im Rahmen der üblichen Verkehrsüberwachung. Den Beamten fielen dabei an dem Auto nach Angaben der LfD „ungewöhnliche Anbauten“ auf, die sich noch vor Ort als Kameras herausstellten. Diese seien unter anderem zur Fehleranalyse verwendet worden und zeichneten das Verkehrsgeschehen rund um das Fahrzeug auf.

Die Aufsichtsbehörde teilte mit, dass „aufgrund eines Versehens“ an dem Auto warnende Magnetschilder mit einem Kamerasymbol und den weiteren vorgeschriebenen Informationen für die datenschutzrechtlich Betroffenen gefehlt haben. Die anderen Verkehrsteilnehmer hätten laut Artikel 13 DSGVO aber etwa über den Zweck der durchgeführten Datenverarbeitung und die Frist der Speicherung der personenbezogenen Informationen aufgeklärt werden müssen.

Bei der weiteren Untersuchung stellten die Prüfer fest, dass Volkswagen keinen Auftragsverarbeitungsvertrag mit dem Unternehmen abgeschlossen hatte, das die Fahrten durchführte. Ein solcher wäre nach Artikel 28 DSGVO nötig gewesen. Ferner hätten die Zuständigen keine Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO durchgeführt, um vorab mögliche Risiken und deren Eindämmung zu bewerten. Schließlich fehlte eine Erklärung der technischen und organisatorischen Schutzmaßnahmen im Verzeichnis der Verarbeitungstätigkeiten, was die Kontrolleure als Verstoß gegen die Dokumentationspflichten nach Artikel 30 DSGVO werteten.

Die Datenschutzbehörde spricht insgesamt von vier Verstößen „mit jeweils niedrigem Schweregrad“, die alle rasch behoben worden seien: VW habe die Mängel, die in keinem Bezug zu Serienfahrzeugen stehen, im Rahmen des Prüfverfahrens unverzüglich abgestellt. Thiel erläuterte: „Die eigentlichen Forschungsfahrten waren datenschutzrechtlich nicht zu beanstanden. Gegen die dabei anfallende Erhebung und Weiterverarbeitung personenbezogener Daten bestehen von unserer Seite keine Bedenken.“ Die Aufsicht habe beim Festlegen der Bußgeldhöhe auch mindernd berücksichtigt, dass die Tests mit den persönlichen Informationen dazu dienten ein Fahrassistenzsystem zu optimieren, dadurch potenziell Unfälle zu vermeiden und so die Sicherheit im Straßenverkehr zu erhöhen.

Aufgrund des grenzüberschreitenden Charakters des Falls beteiligte Thiel vor Erlass des Bußgeldbescheids andere betroffene europäische Datenschutzaufsichtsbehörden im DSGVO-Kooperationsverfahren, die die Entscheidung mittragen. VW hat gemäß der LfD umfassend kooperiert und die Strafe bereits akzeptiert. Die mit über 35 Mio. Euro bislang höchste DSGVO-Sanktion in Deutschland verhängte die Hamburgische Datenschutzbehörde 2020 gegen den Bekleidungshändler H&M. Die EU-weit bisher höchste Strafe traf Amazon Europa in Luxemburg mit 746 Mio. Euro (Die Landesbeauftragte für den Datenschutz Niedersachsen, PE v. 26.07.2022, Datenschutzverstöße im Rahmen von Forschungsfahrten, 1,1 Millionen Euro Bußgeld gegen Volkswagen; Krempl, DSGVO-Verstoß: Volkswagen muss 1,1 Millionen Euro Bußgeld zahlen, www.heise.de 26.07.2022, Kurzlink: https://heise.de/-7190148).

Niedersachsen

Bußgeld gegen Kreditinstitut wegen illegaler Werbung

Die Landesbeauftragte für den Datenschutz (LfD) Niedersachsen hat gegen ein Kreditinstitut eine Geldbuße in Höhe von 900.000 Euro festgesetzt. Das Unternehmen hatte Daten aktiver sowie ehemaliger Kundinnen und Kunden ohne deren Einwilligung ausgewertet. Dazu analysierte es das digitale Nutzungsverhalten und wertete unter anderem das Gesamtvolumen von Einkäufen in App-Stores, die Häufigkeit der Nutzung von Kontoauszugsdruckern sowie die Gesamthöhe von Überweisungen im Online-Banking im Vergleich zur Nutzung des Filialangebots aus und bediente sich hierzu eines Dienstleisters. Ergänzend wurden die Ergebnisse der Analyse mit einer Wirtschaftsauskunftei abgeglichen und von dort angereichert. Ziel war es Kunden mit einer erhöhten Neigung für digitale Medien zu identifizieren und diese adressatengerecht für vertragsrelevante oder werbliche Zwecke verstärkt auf elektronischen Kommunikationswegen anzusprechen. Den meisten Kunden wurden zwar vorab zusammen mit anderen Unterlagen Informationen zugeschickt. Diese ersetzten die notwendigen Einwilligungen allerdings nicht. Der Bußgeldbescheid ist noch nicht rechtskräftig (LfD Niedersachsen, PE 28.07.2022, 900.000 Euro Bußgeld gegen Kreditinstitut wegen Profilbildung zu Werbezwecken).

Nordrhein-Westfalen

VZ klagt gegen Weitergabe von TK-Vertragsdaten

Die Verbraucherzentrale Nordrhein-Westfalen (VZ NRW) hat Klage erhoben gegen die Telekom Deutschland, Vodafone und Telefonica wegen deren Weitergabe von sogenannten „Positivdaten" ihrer Kundinnen und Kunden an Wirtschaftsauskunfteien ohne hierfür eine Einwilligung der Betroffenen eingeholt zu haben. Dadurch würden sie gegen die Datenschutz-Grundverordnung verstoßen; die VZ fordert die Übermittlung der Telekommunikations-(TK-)Daten zu unterlassen.

Die Deutsche Telekom teilte mit, sie übermittle bereits seit Anfang des Jahres 2021 keine Positivdaten mehr an Auskunfteien oder Wirtschaftsauskunfteien. Anlass dafür seien Bedenken der Datenschutzbeauftragten der Länder gewesen (DANA 1/2022, 34): „Wir haben das ganz eingestellt." Von den anderen Unternehmen gab es zunächst keine Stellungnahme. Als Positivdaten werden Informationen bezeichnet, die sich nicht auf ausgebliebene Zahlungen oder sonstiges nicht vertragsgemäßes Verhalten beziehen, sondern darauf, wer wann mit wem einen Vertrag geschlossen hat.

Wolfgang Schuldzinski, Vorstand der Verbraucherzentrale NRW, begründet das Vorgehen: „Die Übermittlung von Positivdaten erscheint auf den ersten Blick vielleicht harmlos, doch jede Information über Verbraucher:innen kann von Unternehmen für spürbare Entscheidungen genutzt werden." Eine Person, die mehrere Mobilfunkverträge habe oder diese häufig wechsele, gelte unter Umständen als weniger vertrauenswürdig und erhalte deswegen keinen Vertrag, auch wenn alle Rechnungen pünktlich bezahlt wurden. Die VZ NRW hatte zunächst die Anbieter Telefónica Germany, Telekom Deutschland und Vodafone erfolglos abgemahnt. Nun hat sie vor dem Landgericht München gegen Telefónica Germany, vor dem Landgericht Köln gegen Telekom Deutschland und vor dem Landgericht Düsseldorf gegen Vodafone Klage erhoben (Positivdaten: Verbraucherzentrale verklagt Telekommunikationskonzerne, www.heise.de 21.07.2022, Kurzlink: https://heise.de/-7186149).

Thüringen

Polizei erhält Bodycams

Nach Pilotprojekten hat der Thüringer Landtag am 14.07.2022 mit großer Mehrheit die flächendeckende Anschaffung von Bodycams am Körper der Polizeibeamten getragene Kameras, beschlossen, deren Einsatz unter Auflagen erlaubt wird. Lediglich die Abgeordneten der FDP stimmten dagegen und kritisierten den damit verbundenen massiven Eingriff in die Bürgerrechte. Die CDU hat schon lange die Einführung von Bodycams im Freistaat gefordert und knüpfte ihre Zustimmung zum Haushalt 2022 unter anderem daran. Insgesamt sind im Etat Thüringens im Jahr 2022 600.000 Euro für die Kameras vorgesehen. In Berlin läuft seit letztem Jahr ein Pilotprojekt, bei dem neben der Polizei auch die Berliner Feuerwehr Bodycams bekommt (DANA 4/2021, 245 f.).

Die Kameranutzung wird sowohl für Bild- als auch für Tonaufnahmen erlaubt ebenso wie die sogenannte Prerecording-Funktion, wobei kontinuierlich ein 30-sekündiger Zeitabschnitt aufgezeichnet und immer wieder überschrieben wird. Drückt der Polizist auf einen Knopf, um eine Aufnahme zu beginnen, werden auch die vergangenen 30 Sekunden gespeichert. Der Einsatz der Kameras in Privaträumen, Anwaltskanzleien und Arztpraxen ist nicht gestattet. In Geschäftsräumen mit Publikumsverkehr sollen Polizisten Aufnahmen anfertigen dürfen, wenn sie Gefahr für Leib und Leben wittern. Zudem müssen die Aufnahmen im Nachgang richterlich überprüft werden. Auch Menschen, gegen die sich eine Amtshandlung richtet, sollen die Aufnahme mit den Kameras verlangen dürfen. Ab 2024 sollen die Kameras automatisch Aufzeichnungen starten, sobald ein Polizist seine Schusswaffe zieht.

Für Innenminister Georg Maier (SPD) ist die Entscheidung des Landtags ein „guter Kompromiss im Sinne der Polizei". CDU-Innenpolitiker Raymond Walk betonte, dass seine Fraktion schon seit Jahren Bodycams gefordert hat: „Heute ist ein guter Tag für mehr Transparenz, aber auch für mehr Sicherheit." Linke und Grüne machten in der Landtagsdebatte dagegen deutlich, dass sie den Körperkameras nur mit Bauchschmerzen zustimmten, und weil die CDU ihre Zustimmung zum Haushalt daran knüpfte. Linken-Innenpolitiker Sascha Bilay sprach von „Erpressung". Grünen-Fraktionschefin Astrid Rothe-Beinlich sagte, ihre Fraktion trage den Kompromiss mit: „Feiern werden wir ihn aber nicht." Den Forderungen der Polizeigewerkschaften Bodycams auch in Privaträumen einsetzen zu dürfen, erteilte sie eine Absage (Sokolov, Polizei Thüringens erhält Bodycams, www.heise.de 14.07.2022, Kurzlink: https://heise.de/-7180378).

Datenschutznachrichten aus dem Ausland

EU

Kritik an Chatkontrolle zwecks Kindesmissbrauchsbekämpfung

Die EU-Kommission hat am 11.05.2022 ihre Pläne für eine umfassende Chatkontrolle zur Bekämpfung von Kindesmissbrauch auf den Weg gebracht. Damit sollen Hoster und Messengerdienste dazu gezwungen werden können Fotos und Videos von Kindesmissbrauch mit spezieller Software vollautomatisiert aufzuspüren – auch in privaten und verschlüsselten Nachrichten ihrer Nutzer. Die zuständige Innenkommissarin Ylva Johansson meinte: „Europa nimmt mit diesem Gesetz weltweit eine Führungsrolle im Kampf gegen sexuellen Missbrauch von Kindern ein." Allein im Jahr 2021 seien 85 Mio. Fotos und Videos im Internet zu sexuellem Missbrauch entdeckt worden. Die Wachstumsraten seien erschütternd, gerade bei Kindern zwischen 7 und 10 Jahren: „Wir scheitern heute daran Kinder zu schützen." Europa sei Schwerpunkt dieser Kriminalität. Die Koordination mit den Behörden der Mitgliedsländer soll eine bei Europol angesiedelte „EU-Zentralstelle" übernehmen.

• Das geplante Gesetz

Große Plattformen wie Facebook hatten Privatnachrichten ihrer Nutzer bis Dezember 2020 freiwillig nach Missbrauchsdarstellungen gescannt. Treffer wurden an das US-Zentrum für vermisste und ausgebeutete Kinder gegeben, wo sie geprüft und gegebenenfalls an Verfolgungsbehörden weitergegeben wurden. Weil für Ende 2020 in der EU zeitweise die rechtliche Grundlage fehlte, einigten sich die EU-Staaten 2021 auf eine Übergangsregelung, die spätestens nach drei Jahren ausläuft. Das EU-Parlament hatte im Juli 2021 per Eilverordnung Ausnahmen von der Anwendung einiger Bestimmungen der E-Privacy-Richtlinie eingeführt. Facebook, Google, Microsoft und andere Diensteanbieter ohne durchgängige Verschlüsselung dürfen und müssen demnach gemäß Art. 10 des 134-seitigen Entwurfs private Nachrichten ihrer Nutzer wieder rechtmäßig nach Darstellungen sexuellen Missbrauchs Minderjähriger scannen (vgl. DANA 1/2021, 50).

Das neue Gesetz soll die Digitalunternehmen verpflichten eine Risikoabschätzung vorzulegen. Dabei soll es einerseits um die Verbreitung strafbarer Bildinhalte mit sexueller Gewalt gegen Kinder gehen, andererseits auch um Anzeichen von „Grooming", also die Versuche von Missbrauchstätern sich Kindern im Netz zu nähern und ihr Vertrauen zu gewinnen. Sollte ein relevantes Risiko festgestellt werden, kann die nationale Aufsichtsbehörde einen „Kontrollauftrag" erwirken. Mit welcher Technologie die Kommunikation kontrolliert wird, soll in Absprache mit der neuen EU-Agentur „Zentrum zur Bekämpfung von sexualisierter Gewalt gegen Kinder und Jugendliche" festgelegt werden. Gemäß Johansson ist das Gesetz im Prinzip „technologieneutral" angelegt. Eingesetzt werden sollen offensichtlich automatisierte lernfähige Systeme. Es solle die Technologie gewählt werden, die am wenigsten in die Privatsphäre der Nutzenden eindringe. So wie es möglich sei mit einem Magneten die Nadel im Heuhaufen zu finden, sei es auch möglich kriminelle Inhalte aus Privatnachrichten herauszufiltern.

• Kritik

Datenschützer, Bürgerrechtler und Forscher protestieren seit Monaten gegen das Vorhaben, das Teil der „EU-Strategie zum Schutz und zur Stärkung von Kindern in der Online-Welt" ist. 47 Organisationen, darunter die DVD, schrieben einen Brandbrief und kritisierten die damals noch geplante „anlasslose Massenüberwachung" (vgl. DANA 2/2022, 100 f.). Die Technik, Bilder anhand ihres digitalen Fingerabdrucks zu erkennen, ist fehleranfällig. Weil sie Kontext und Details der Bilder nicht detektieren kann, wird es hunderttausende falsche Treffer geben. Bis das auffällt, sind private völlig legale Bilder schon in der Hand der EU-Behörde. Die Software garantiert auch nicht, dass erkannt wird, ob ein Mensch auf einem Bild minderjährig oder gerade 18 Jahre alt ist und dass es sich bei den Bildern um Straftaten handelt. Das neue System würde eine Standleitung in das Intimleben vieler junger Menschen schaffen.

Der Chaos Computer Club (CCC) spricht von einer „fundamental fehlgeleiteten Technologie" und warnte vor allem vor dem sog. Client-Side-Scanning, also der Überwachung der Daten auf den Endgeräten der Nutzer, die im Gesetz nicht ausgeschlossen wird. Ella Jakubowska, politische Beraterin bei der Bürgerrechtsorganisation European Digital Rights (EDRi), meinte: Die Vorstellung, dass die private Kommunikation der mehreren hundert Millionen EU-Bürger „wahllos und generell rund um die Uhr gescannt wird, ist beispiellos". Über das Scannen von Inhalten hinaus befürchten Aktivisten wie auch Tech-Firmen, dass die Kommission faktisch Hintertüren bei Ende-zu-Ende-verschlüsselten Messaging-Diensten vorschreiben könnte. Laut EDRi öffnet die Kommission „die Tür für ein breites Spektrum an autoritären Überwachungstaktiken". Spezifische Webinhalte könnten zudem beim verschlüsselten Webprotokoll HTTPS nicht gezielt geblockt werden.

WhatsApp-Chef Will Cathcart zeigte sich auf Twitter „unglaublich enttäuscht" über diese „furchtbare Idee", dass die geplante EU-Verordnung „die Ende-zu-Ende-Verschlüsselung nicht schützt". Der hannoversche E-Mail-Anbieter Tutanota will „alle Rechtsmittel" gegen ein solches Gesetz ausschöpfen. Der Kryptologe Matthew Green verwies auf Probleme mit der Meinungsfreiheit. Hinauslaufen dürfte es ihm zufolge auf einen ähnlichen Ansatz wie bei den nicht weniger umkämpften „SpyPhone"-Plänen von Apple. Und selbst der Deutsche Kinderschutzbund hält die Pläne für „unverhältnismäßig und nicht zielführend".

Auch in der deutschen Politik gibt es parteiübergreifenden Gegenwind. Der digitalpolitische Sprecher der SPD Jens

Zimmermann meinte: „Unfassbar, was da aus Brüssel kommt. Das gehört eher nach Russland als nach Europa." Der grüne MdB Konstantin von Notz spricht von einem „gefährlichen Irrweg" und hat „massive Zweifel", ob dieser mit der Verfassung vereinbar sei: „Aus diesem Grund haben sich Grüne, SPD und FDP im Koalitionsvertrag gegen dieses Vorhaben ausgesprochen." Die Linke Anke Domscheit-Berg wirft der Bundesregierung „Naivität" vor. Innenministerin Nancy Faeser sei von der EU-Bekanntmachung „offensichtlich völlig überrascht" gewesen. Besserer Kinderschutz sei wichtig, dafür gebe es indes effektivere Methoden.

• Das weitere Verfahren

Sowohl das Europaparlament als auch die Mitgliedstaaten müssen dem Entwurf zustimmen. Es dürfte in beiden Institutionen heftige Debatten geben. Im EU-Parlament gibt es Widerstand. Patrick Breyer hat bereits Unterlassungsklage gegen die Facebook-Mutter Meta vor dem Amtsgericht Kiel eingereicht, da der Betreiber des sozialen Netzwerks freiwillig schon jetzt eine Chatkontrolle durchführe. Moritz Körner, Innenexperte der FDP im EU-Parlament, monierte, dass die Kommission Websperren „verpflichtend in allen EU-Staaten einführen und mit Hilfe einer europäischen Big-Brother-Agentur die Onlinewelt überwachen" will. Kämen Kommissionspräsidentin Ursula von der Leyen (CDU) und Johansson mit der neuen „Zensursula"-Initiative durch, „wäre das digitale Briefgeheimnis tot". Unternehmen dürften nicht gezwungen werden Polizei zu spielen, ihre Kunden auszuspionieren und beim Staat zu melden: „Diese Stasi 2.0 ist abzulehnen." Die Grüne Alexandra Geese meinte: „Über das Ziel, sexualisierte Gewalt gegen Kinder zu verfolgen, herrscht absoluter Konsens. Aber die Wahl der geeigneten Mittel ist haarsträubend. Wir dürfen nicht aus blindem Aktionismus einen Freifahrtschein für das Überwachen der gesamten privaten Kommunikation von Menschen in der EU erteilen." 20 EU-Parlamentarier fast aller Fraktionen hatten zuvor gemeinsam Alarm geschlagen: Es drohten chinesische Verhältnisse. Die Kritiker der Massenüberwachung fordern stattdessen eine bessere personelle und finanzielle Ausstattung von Polizei, Ermittlungsbehörde und Jugendämtern (Krempl, EU-Chatkontrolle: „Europäische Big-Brother-Agentur", www.heise.de 11.05.2022, Kurzlink: https://heise.de/-7082775; Brühl/ Kelnberger, EU will Chats überwachen lassen, SZ 12.05.2022, 1; Brühl, Stoppt den großen Scanner, SZ 12.05.2022, 17).

EU

Vorschlag für Europäischen Gesundheitsdatenraum vorgestellt

Stella Kyriakides, EU-Gesundheitskommissarin, und Margaritis Schinas, Vizepräsident der Europäischen Kommission, stellten am 03.05.2022 den Vorschlag der EU-Kommission für eine Verordnung zum Europäischen Gesundheitsdatenraum (European Health Data Space – EHDS) vor und sparten dabei nicht mit großen Worten. Dies sei „revolutionär", ein „Game Changer", „wichtig und notwendig". Mit diesem Datenraum wolle man, so Schinas, die bestehenden Ungleichheiten in den Gesundheitssystemen verringern: „Gesundheitsdaten sind Macht", aus der man allerdings bisher zu wenig mache. Der Gesundheitsdatenraum sei sowohl „gesundheitspolitisch als auch ökonomisch sinnvoll".

• Der Vorschlag

Die Grundzüge des EHDS bestehen darin, dass jeder EU-Bürger digital auf die eigenen Gesundheitsdaten zugreifen und diese kontrollieren können soll. Auch Ärzten und anderem medizinischen Personal soll der Zugang zu Gesundheitsdaten erleichtert werden, indem eine sowohl fach- als auch länderübergreifende Interoperabilität der Daten gewährleistet wird (primäre Nutzung). So soll eine spanische Orthopädin auf das MRT eines rumänischen Patienten zugreifen können, das dieser im Urlaub in einem niederländischen Krankenhaus machen ließ. Zudem sollen Forschung, Industrie sowie öffentliche Gesundheitsinstitutionen stärker von aggregierten digitalen Gesundheitsdaten profitieren (sekundäre Nutzung) und zu diesen Zugang erhalten.

Gemäß dem Entwurf der Verordnung soll den Bürgern der Zugang über ein EU-weit elektronisches interoperables Format geboten werden, das Kontrollmöglichkeiten über die Speicherung und Weitergabe der Gesundheitsdaten (z.B. Rezepte, Laborergebnisse, Entlassberichte, Impfnachweise, aber auch von Wellness-Apps) gewährt. Das schließt auch ein bestimmten Akteuren den Zugriff zu verwehren, Daten hinzuzufügen und andere zu löschen.

Die EU-Kommission will bei dem Aufbau der digitalen Infrastruktur auf bereits bestehende Ansätze setzen. Schon jetzt können über das Modellprojekt „MyHealth@EU" Ärzte und Apotheken aus insgesamt zehn EU-Mitgliedstaaten länderübergreifend auf Patientenbriefe beziehungsweise Verschreibungen zugreifen. In diesem Rahmen soll künftig jeder Mitgliedstaat eine nationale Kontaktstelle für elektronische Gesundheitsdienste benennen und sämtliche Gesundheitsdienstleister mit ihr verbinden.

Für die sekundäre Nutzung durch Wissenschaft und Industrie sollen die Bestimmungen der Datenschutz-Grundverordnung und des (vorgeschlagenen) Data Governance Act gelten. Nur Daten, die für den jeweiligen Zweck gebraucht werden, sollen in anonymisierter Form auf Antrag bereitgestellt werden. Unter engen Voraussetzungen sollen auch Daten in pseudonymisierter Form bereitgestellt werden. Ein sog. „European Health Data Space Board", bestehend aus Mitgliedern der oben genannten Kontaktstellen sowie von Kommissionsmitgliedern und unter Einbeziehung von Patientenorganisationen und Datenschutzbehörden soll den Aufbau des EHDS begleiten und eine übergeordnete Koordinierungsfunktion übernehmen.

• Finanzierung

Gemäß Kyriakides soll die Verordnung einen „gesetzlichen Rahmen" liefern. Für den Großteil der Umsetzung – also etwa den Zugang zu persönlichen Gesundheitsdaten – seien die Mitgliedsstaaten verantwortlich. Allerdings habe man das Gefühl, dass in dieser Frage große Einigkeit und großer Wille herrsche. Bis 2025 soll der Europäische Ge-

sundheitsdatenraum Realität sein. Der Vorschlag muss nun vom EU-Parlament und dem Ministerrat behandelt werden.

Die EU-Kommission hofft, dass durch den besseren Zugang und Austausch von Gesundheitsdaten im Gesundheitswesen, z.B. weil aufwändige Tests und Untersuchungen nicht mehrmals durchgeführt werden müssten, 5,5 Mrd. Euro über einen Zeitraum von zehn Jahren eingespart werden können. Weitere 5,4 Mrd. Euro könnten durch die sekundäre Nutzung eingespart werden.

Die Finanzierung soll größtenteils aus der sog. Aufbau- und Resilienzfazilität, dem Kernstück des Konjunkturpakets „NextGenerationEU“, das in Folge der Coronakrise geschnürt wurde, erfolgen. 12 Mrd. Euro stünden aus diesem Topf für Investitionen in die digitale Gesundheit bereit. Darüber hinaus will die EU-Kommission einmalig 810 Mio. Euro bereitstellen. Weitere 280 Mio. Euro stünden aus dem EU4Health-Programm zur Verfügung. Der Rest würde über die Investionsprogramme „Digital Europe Programme“, „Connecting Europe Facility“ und „Horizon Europe“ finanziert.

• Nationale Umsetzung

Bitkom, der Branchenverband der deutschen Informations- und Telekommunikationsbranche, lobte den Vorschlag der Kommission und forderte für Deutschland mehr Tempo bei der elektronischen Patientenakte, dem Ausbau der Telematik und der Interoperabilität. In diesem Zusammenhang sei wichtig, dass das im Koalitionsvertrag geplante deutsche Gesundheitsdatennutzungsgesetz schnell und in Einklang mit den europäischen Regelungen auf den Weg gebracht werde.

Mario Brandenburg, Sprecher für Forschung, Technologie und Innovation der FDP-Bundestagsfraktion, begrüßte den EU-Vorschlag als „richtigen Schritt hin zu einem digital vernetzten Europa“. Die Kommission habe „ein patient:innenzentriertes Konzept vorgestellt, welches datengetriebene Innovationen stärkt und zugleich den Menschen die Entscheidungshoheit über die Verwendung ihrer sensiblen Gesundheitsdaten selbst in die Hand gibt“. Offen bleibe, wie die Gesundheitsdaten sicher gespeichert werden sollen sowie wie eine differenzierte Freigabe der individuellen Daten für unterschiedliche Zwecke erfolgen soll, was von den Mitgliedsstaaten zu beantworten sei, in deren Hoheit die Umsetzung des Zugangs zu den Gesundheitsdaten liege.

Dass es an dieser Stelle Klärungsbedarf gibt, zeigt u.a. die Klage des Vereins Gesellschaft für Freiheitsrecht (GFF), der mitteilte Eilanträge gegen das Sammeln von Gesundheitsdaten der Krankenkassen auf der Grundlage des Digitale-Versorgung-Gesetzes (DVG) bei den Sozialgerichten Berlin und Frankfurt eingereicht zu haben. Das DVG sieht vor, dass die gesetzlichen Krankenkassen Gesundheitsdaten ihrer Versicherten pseudonymisiert sammeln, um sie der Forschung zur Verfügung zu stellen. Laut GFF sind die Daten jedoch nicht ausreichend vor einer Reidentifizierung geschützt (Böldt, EU stellt Weichen für Gesundheitsdatenraum, Tagesspiegel Digitalisierung & KI 04.05.2022).

Spanien

Pegasus-Einsatz provoziert Regierungskrise

Die Amtstätigkeit von Paz Esteban, die 2020 als erste Frau an die Spitze des spanischen Geheimdienstes Centro Nacional de Inteligencia (CNI) berufen worden war, wurde von ihrer Vorgesetzten, der Verteidigungsministerin Margarita Robles, Anfang Mai 2022 beendet. Die Behörde wird künftig von der bisherigen Staatssekretärin im Verteidigungsministerium, Esperanza Casteleiro (65) geleitet, die seit fast 40 Jahren im CNI arbeitet. Zuvor hatte Esteban vor Journalisten eingeräumt, dass ihre Behörde katalanische Unabhängigkeitsbefürworter mit Hilfe der israelischen Spionage-Software Pegasus ausgespäht habe. 18 katalanische Aktivisten und Politiker seien im Herbst 2019 von ihren Beamten abgehört worden. Für jeden dieser Einzelfälle hatte Esteban am 05.05.2022 in einer parlamentarischen Kontrollkommission eine richterliche Erlaubnis vorgelegt. Für den Rest der insgesamt 63 mutmaßlich mit Hilfe von Pegasus bespitzelten Separatisten und Personen aus deren Umfeld habe Esteban, so die Presse, keine Verantwortung übernommen. Man habe damals erneut die Gefahr einer drohenden Abspaltung Kataloniens gesehen. Richter hätten die Überwachung der Telefone angeordnet.

Die im „Catalangate“ eingesetzte umstrittene Spähsoftware Pegasus der israelischen NSO Group war auf Geräten katalanischer Politiker entdeckt worden. Bereits Mitte April hatte die kanadische Forschungsgruppe Citizen Lab einen Bericht veröffentlicht, wonach die Mobiltelefone von 63 katalanischen Unabhängigkeitsbefürwortern in den Jahren 2017 bis 2020 mit Pegasus ausgespäht wurden. Betroffen sind drei ehemalige katalanische Regionalpräsidenten, die Anführer der großen zivilgesellschaftlichen Separatistenorganisationen, die Anwälte mehrerer angeklagter Politiker, darunter der Anwalt von Carles Puigdemont, Gonzalo Boye, ebenso Puigdemonts Ehefrau. Der letzte Angriff auf ein katalanisches Smartphone erfolgte laut Citizen Lab am 27.06.2020 gegen den linksrepublikanischen Europaabgeordneten Jordi Solé. Der Hersteller NSO betont, die Software werde nur an Regierungsorganisationen verkauft.

Katalanische Separatisten, auf deren Stimmen die Minderheitsregierung von Ministerpräsidenten Pedro Sánchez angewiesen ist, forderten deshalb nicht nur die Entlassung Estebans, sondern auch von Robles. Der Sozialist Sánchez regiert mit der linkspopulistischen Partei Podemos. Seine Legitimation als Regierungschef, der nach der harten Hand seines konservativen Vorgängers Mariano Rajoy auf den Dialog mit Katalonien setzt, ist angeknackst. Bislang konnte Sánchez auf die Stimmen der 13 Abgeordneten der katalanischen Esquerra Republicana (ERC) zählen, die in Barcelona den Regionalpräsidenten Pere Aragonès stellt. Der 39 Jahre alte Aragonès ist seit September Regierungschef im Nordosten Spaniens und gilt als gemäßigter Separatist. Er hatte sich aus dem Schatten seiner deutlich aggressiveren Vorgänger Quim Torra und Carles Puigdemont gelöst. Sein Name stand auch auf der Liste der Zielpersonen im Bericht des Citizen Lab. Aragonès forderte weitere Konsequenzen aus der Spionage-Affäre. Neben der Entlassung von Robles fordert er insbesondere die Einsetzung einer Untersuchungskommission und die Freigabe der Akten.

Etwas später wurden auch Hinweise auf Pegasus in Smartphones von Sánchez, Robles und Innenminister Fernando Grande-Marlaska gefunden, die demnach seit Frühjahr 2021 unter technischer Beobachtung standen. Dies war erst nach etwa einem Jahr bemerkt worden, weshalb der CNI noch stärker unter Druck geriet. Weshalb diese Bespitzelung erst nach der Offenlegung der Beobachtung der katalanischen Politiker bekannt gemacht wurde, ist eine offene Frage. In spanischen Medien wurde spekuliert, Marokko könne hinter dieser Aktion stecken. Dabei wurden nach Angaben der Regierung in Madrid rund 3,6 Gigabyte Daten von Sanchez' Handy gestohlen.

Sánchez steckt in der Zwickmühle: Er ist auf die Unterstützung der Linksrepublikaner angewiesen; es soll aber nicht so aussehen, als würde er vor Aragonès einknicken, was ihm die konservative Opposition von der Partido Popular vorwirft. Der Präsident habe den Kopf der Geheimdienstchefin als „Willkommensbrief“ gesendet, so deren Chef Alberto Nunez Feijoo (Janker/Kelnberger, Unfreundliche Annäherung, SZ 20.04.2022, 6; Janker, Aragonès will „Köpfe rollen sehen, SZ 23./24.04.2022, 8; Spähangriff auf Separatisten, Der Spiegel Nr. 17 23.04.2022, 75; Pegasus-Spyware: Spaniens Geheimdienst räumt Bespitzelung von Separatisten ein, www.heise.de 05.05.2022, Kurzlink: https://heise.de/-7077118; Kirchner, Nach Bespitzelung von Smartphones: Spaniens Geheimdienstchefin tritt ab, www.heise.de 10.05.2022, Kurzlink: https://heise.de/-7081100; Pegasus-Spyware: Spaniens Geheimdienstchefin geschasst, Deutsche Welle vom 10.05.2022, https://p.dw.com/p/4B5yR; Janker, www.dw.com/de 10.05.2022; Enttarnte Spione SZ 14./15.05.2022, 6).

Polen

Frauen fürchten Pflicht zur Schwangerschaftsregistrierung

Der polnische Gesundheitsminister Adam Niedzielski hat am 03.06.2022 eine Verordnung unterzeichnet, die eine heftige Debatte auslöste: Diese sieht eine Registrierung für Schwangere vor, was sich nach einem obligatorischen Meldesystem und nach Überwachung anhört. Aktivistinnen und Juristen fürchten, Frauen müssten bald Rechenschaft über den Verlauf ihrer Schwangerschaft ablegen, sich vielleicht unangenehmen Fragen stellen. Abtreibung ist in Polen praktisch verboten, auch dann, wenn der Fötus stark geschädigt ist. Nur, wenn das Leben der Mutter offensichtlich in Gefahr ist oder etwa eine Vergewaltigung zur Schwangerschaft führte, ist die Abtreibung erlaubt.

Niedzielski und seine Ministeriumsmitarbeiter beteuern, es handle sich lediglich um die Umsetzung einer EU-Richtlinie, nach der Patientendaten durch eine zentrale Registrierung schnell und unkompliziert zur Verfügung stehen sollen. In Deutschland wird deshalb die elektronische Krankenakte eingeführt. Nur Patienten und Ärzte haben darauf Zugriff, und so soll es auch in Polen sein. Die polnische Diskussion dreht sich aber nicht – wie in Deutschland – um Datensicherheit oder mögliche Datenzugriffe von Arbeitgebern oder Krankenkassen. Vielmehr herrscht die Sorge vor, die Angaben könnten von Ermittlern genutzt werden – etwa um Schwangerschaftsabbrüche zu verfolgen oder grundsätzlich Druck auf Schwangere auszuüben.

Agnieszka Dziemianowicz-Bąk, Abgeordnete der Linken, erklärte auf einer Pressekonferenz, dass die Erfassung der Daten „in einem zivilisierten Land“ eigentlich kein Problem sei: „Aber in einem Land mit einem fast vollständigen Abtreibungsverbot muss uns das erschrecken.“ Oppositionsführer Donald Tusk von der konservativen Bürgerplattform PO sagte, das Register solle offensichtlich der Kontrolle der Frauen dienen. Er versprach im Falle eines Wahlsieges bei den Parlamentswahlen im Herbst 2023 Abtreibungen bis zur zwölften Woche zu legalisieren. Treibende Kraft hinter einer mit 100.000 Unterschriften eingeforderten Gesetzinitiative im Sejm, die diese Legalisierung jetzt schon durchsetzen möchte, ist Marta Lempart, Anführerin des „Strajk Kobiet“ (Frauenstreik). Sie befürchtet, dass das sogenannte Schwangerschaftsregister dazu führen kann, dass schwangere Frauen medizinische Behandlungen meiden. Dziemianowicz-Bąk meinte: „Polnische Frauen werden nicht mehr schwanger, aus Angst in irgendeiner Situation zur Geburt gezwungen zu werden.“ Tatsächlich ist die Geburtenrate in Polen angesichts der seit Monaten stattfindenden Auseinandersetzungen zum Abtreibungsverbot mit statistisch 1,39 Kindern pro Frau äußerst niedrig (Grossmann, Die kontrollierte Frau, SZ 10.06.2022, 9).

Großbritannien

Queen's Speech kündigt neues Datenschutzgesetz an

In ihrer von Prinz Charles vorgetragenen, jährlichen Ansprache („Queen's Speech“) an das Parlament am 10.05.2022 hat die englische Königin 38 neue Gesetze angekündigt – darunter eines zum Datenrecht: „Das Datenschutzsystem des Vereinigten Königreichs wird reformiert.“ Man wolle die „Vorteile des Brexits nutzen, um ein Datenrechtssystem von Weltklasse zu schaffen, das es uns ermöglicht einen neuen wachstumsfördernden und vertrauenswürdigen britischen Rahmen für den Datenschutz zu schaffen“. Bereits 2021 hatte der britische Digitalminister Oliver Dowden angekündigt, dass man sich von den Vorgaben der DSGVO emanzipieren und beim Datenschutz eine eigene Linie verfolgen wolle (DANA 4/2021, 253 ff.).

Das Information Commissioner's Office, die oberste Datenschutzbehörde des Vereinigten Königreichs, müsse dadurch modernisiert werden, dass sie die Fähigkeiten und Befugnisse habe gegen Organisationen vorzugehen, die gegen Datenschutzgesetze verstoßen. Die Behörde müsse aber gegenüber dem Parlament und der Öffentlichkeit stärker rechenschaftspflichtig sein. Die Industrie solle stärker beteiligt werden an „Smart Data“-Programmen, die Bürgern und kleinen Unternehmen mehr Kontrolle über ihre Daten geben. Der Gesetzentwurf werde auch denjenigen helfen, die eine Behandlung im Gesundheitswesen benötigen, indem sie den angemessenen Zugang zu Daten im

Gesundheitswesen und in der Sozialfürsorge verbessern.

Als wichtigste Vorteile des geplanten Gesetzes nennt die Queen's Speech die Steigerung der Wettbewerbsfähigkeit und Effizienz britischer Unternehmen durch Verringerung der Belastungen, die sie zu tragen haben, z.B. durch die Schaffung eines Datenschutzrahmens, der sich auf die Ergebnisse des Datenschutzes konzentriere und nicht auf das Abhaken von Kästchen. Die weiteren angesprochenen Punkte:

- Das Gesetz soll sicherstellen, dass Daten genutzt werden können, um die Bürger zu stärken und ihr Leben zu verbessern durch eine effektivere Bereitstellung öffentlicher Gesundheits-, Sicherheits- und anderer Dienstleistungen.
- Schaffung eines klareren rechtlichen Umfelds für die Nutzung personenbezogener Daten, das die verantwortungsvolle Innovation und den wissenschaftlichen Fortschritt vorantreibt.
- Sicherstellung, dass die Regulierungsbehörde angemessene Maßnahmen gegen Organisationen ergreift, die die Datenrechte verletzen, und dass die Bürger mehr Klarheit über ihre Rechte haben
- Vereinfachung der Regeln für die Forschung, um die Position des Vereinigten Königreichs als wissenschaftliche und Technologie-Supermacht zu festigen.

Die Queen's Speech enthält weitere geplante Gesetze, die IKT- und digitale Themen betreffen, etwa ein Gesetz über digitale Märkte, Wettbewerb und Verbraucherschutz sowie ein Gesetz über Produktsicherheit und Telekommunikationsinfrastruktur (Roos, „The Queen's Speech": Neues Datenschutzgesetz angekündigt, www.heise.de 11.05.2022, Kurzlink: https://heise.de/-7081999).

Großbritannien

Bußgeld gegen Clearview AI

Das britische Information Commissioner's Office (ICO) hat die US-Firma Clearview AI mit einer Geldstrafe in Höhe von 7.552.800 Pfund (ca. 8,9 Millionen Euro) belegt und verpflichtet ihre britischen Daten in der Gesichtserkennungsdatenbank zu löschen. Das Unternehmen hat gegen die britischen Datenschutzgesetze verstoßen, indem es Bilder von Personen aus dem Vereinigten Königreich und anderen Ländern, die im Internet und in sozialen Medien gesammelt wurden, zur Erstellung einer globalen Online-Datenbank verwendet, die für die Gesichtserkennung genutzt werden kann.

Die ICO ist als unabhängige Behörde des Vereinigten Königreichs für die Wahrung der Informationsrechte und des Datenschutzes zuständig. In ihrer Vollstreckungsmitteilung forderte sie gemäß ihrer Mitteilung vom 23.05.2022 Clearview AI auf die Beschaffung und Verwendung personenbezogener Daten britischer Bürger, die im Internet öffentlich zugänglich sind, einzustellen und deren Daten aus seinen Systemen zu löschen.

Eine gemeinsame Untersuchung mit dem Office of the Australian Information Commissioner (OAIC) befasste sich mit der Verwendung von Personenbildern durch Clearview AI, das Auslesen von Daten aus dem Internet und die Verwendung der biometrischen Daten zur Gesichtserkennung. Demnach hat Clearview AI mehr als 20 Milliarden Bilder von Gesichtern und Daten aus öffentlich zugänglichen Informationen im Internet und auf Social-Media-Plattformen in der ganzen Welt gesammelt, um eine Online-Datenbank zu erstellen. Die Menschen wurden nicht darüber informiert, dass ihre Bilder gesammelt oder verwendet wurden.

John Edwards, der britische Informationsbeauftragte, erläuterte: „Das Unternehmen ermöglicht nicht nur die Identifizierung dieser Personen, sondern überwacht auch ihr Verhalten und bietet dies als kommerzielle Dienstleistung an. Das ist inakzeptabel. Deshalb haben wir gehandelt, um die Menschen im Vereinigten Königreich zu schützen, indem wir dem Unternehmen eine Geldstrafe auferlegt und einen Vollstreckungsbescheid erlassen haben. Die Menschen erwarten, dass ihre persönlichen Daten respektiert werden, unabhängig davon, wo auf der Welt ihre Daten verwendet werden. Deshalb brauchen globale Unternehmen eine internationale Durchsetzung. Die Zusammenarbeit mit Kollegen auf der ganzen Welt hat uns geholfen diese Maßnahme zu ergreifen und die Menschen vor solch aufdringlichen Aktivitäten zu schützen."

Kunden von Clearview, einschließlich der Polizei, können das Bild einer Person in die App des Unternehmens hochladen, damit es dann auf eine Übereinstimmung mit allen Bildern in der Datenbank überprüft wird. Die App liefert darauf eine Liste von Bildern, die ähnliche Merkmale aufweisen wie das hochgeladene Foto, mit einem Link zu den Websites, von denen diese Bilder stammen. Zwar bietet Clearview AI seine Dienste nicht mehr für britische Organisationen an, hat aber Kunden in anderen Ländern, so dass immer noch personenbezogene Daten von im Vereinigten Königreich ansässigen Personen verwendet werden.

Kurz zuvor war Clearviews umstrittene Gesichtserkennungs-App für private US-Firmen verboten worden. Nach einer gerichtlichen Einigung mit einer Bürgerrechtsorganisation darf Clearview AI die biometrischen Daten seiner Gesichtserkennungssoftware in den USA nicht mehr an Unternehmen und private Akteure verkaufen. Auch das EU-Parlament fordert ein Aus für biometrische Massenüberwachung und Social Scoring. Ermittlern soll laut der Anfang Oktober 2021 angenommenen Resolution untersagt werden private Gesichtserkennungsdatenbanken zu nutzen, wie sie etwa Clearview AI zusammengetragen hat. Das auf biometrische Gesichtserkennung spezialisierte US-Unternehmen sieht sich trotz zahlreicher rechtlicher Querelen und internationaler Kritik auf massivem Expansionskurs. Clearview will seine Datenbank mit 100 Milliarden Gesichtsfotos füllen und binnen eines Jahres „fast jeden Menschen auf der Welt" identifizieren und auch Firmenmitarbeiter überwachen können. Die Ukraine setzt Clearview AI bereits zur Identifizierung Gefallener ein und will so getötete russische Soldaten identifizieren (Knobloch, Clearview: Britische Aufsichtsbehörde verhängt Millionenstrafe, www.heise.de 24.05.2022, Kurzlink: https://heise.de/-7103797).

USA

Strafzahlung für Twitter wegen Datenmissbrauch für Werbezwecke

Der Online-Dienst Twitter hat laut Vorwürfen der US-Regierung Kontaktdaten von Nutzern für Werbung verwendet und muss deshalb 150 Millionen US-Dollar (etwa 140 Millionen Euro) zahlen. Twitter einigte sich auf diese Strafzahlung, um eine Datenschutzklage amerikanischer Behörden beizulegen.

In der am 25.05.2022 veröffentlichten Klageschrift verweisen die Handelsbehörde FTC (Federal Trade Commission) und das Justizministerium darauf, dass Twitter die Nutzer um ihre Telefonnummern und E-Mail-Adressen mit der Begründung gebeten habe, man könne damit besser ihre Accounts absichern. Online-Dienste greifen zu E-Mails oder Nachrichten an Handy-Nummern zum Beispiel zur Anmeldung auf neuen Geräten, bei vergessenen Passwörtern oder um gesperrte Profile wieder freizuschalten. Twitter hat die Daten aber gemäß der Klage auch verwendet, um Nutzern personalisierte Werbung anzuzeigen. Damit seien die für andere Zwecke erhobenen Kontaktinformationen missbraucht worden.

Zwischen Mai 2013 und September 2019 haben demnach mehr als 140 Millionen Nutzende ihre Telefonnummern oder E-Mail-Adressen mit Twitter geteilt. Die US-Regierung sieht in der Vorgehensweise des Dienstes einen Verstoß gegen eine Einigung aus dem Jahr 2011, bei der sich Twitter unter anderem zu Transparenz beim Datenschutz verpflichtet hatte. Der Dienst wurde von der Regierung deshalb als Wiederholungstäter betrachtet, was die Tür für eine hohe Zahlung öffnete.

Mit 150 Mio. US-Dollar kommt Twitter allerdings deutlich günstiger davon als Facebook im Jahr 2019. Damals warfen US-Behörden dem weltgrößten Online-Netzwerk ebenfalls vor früher eingegangene Datenschutz-Verpflichtungen verletzt zu haben. Facebook zahlte fünf Milliarden Dollar und stimmte einer strikteren Datenschutz-Aufsicht zu (DANA 3/2019,164 f.). Auch Twitter muss nun unter anderem den Datenschutz von durch die FTC benannten Experten prüfen lassen und der Behörde Zwischenfälle binnen 30 Tagen melden. Außerdem soll Twitter ein Verfahren zur sicheren Anmeldung anbieten, das ohne eine Telefonnummer funktioniert.

Die Strafzahlung und die neuen Auflagen kamen mitten im Übernahmeversuch des Tech-Milliardärs Elon Musk bei Twitter. Der Deal lief nicht rund: Musk hatte die Übernahmevereinbarung zuletzt für ausgesetzt erklärt und dies mit dem Verdacht begründet, dass der Anteil von Spam- und Bot-Accounts höher sei als die in offiziellen Berichten genannten Schätzungen von weniger als 5%. Aus Sicht der Plattform kann Musk das Geschäft jedoch nicht einseitig auf Eis legen; Twitter beharrt auf dem Kaufvertrag (Twitter missbraucht Kundendaten, SZ 27.05.2022, 20; Twitter: Strafzahlung nach Datenschutz-Vorwürfen, Musk schichtet Finanzierung um, www.heise.de 26.05.2022, Kurzlink: https://heise.de/-7123327).

USA

Clearview verzichtet auf Vermarktung bei Privatunternehmen

Nach einer gerichtlichen Einigung darf Clearview AI die biometrischen Daten seiner umstrittenen Gesichtserkennungssoftware in den USA nicht mehr an Unternehmen und private Akteure verkaufen (vgl. DANA 1/2022, 45). Das hat ein Vergleich mit der Bürgerrechtsorganisation ACLU (American Civil Liberties Union) von Illinois und Nebenklägern wie der Alliance Against Sexual Exploitation vor dem Hintergrund des 2008 in Kraft getretenen Datenschutzgesetzes von Illinois „Biometric Information Privacy Act (BIPA)“ ergeben. Die Entscheidung ist über Illinois hinaus für die gesamte USA gültig. Staatliche Organisationen dürfen Clearviews App jedoch – außer in Illinois – weiter verwenden. Dort gilt für einen Zeitraum von 5 Jahren ein Verbot des Verkaufs der App an Strafverfolgungs- und Polizeibehörden.

Im Jahr 2020 hatte die ACLU eine Klage eingereicht und Clearview AI vorgeworfen gegen ein Urteil von Illinois zu verstoßen. Nach dem BIPA dürfen „private Einrichtungen oder Einzelpersonen“ ohne Einwilligung der Personen nicht mehr deren biometrische Daten sammeln oder verwenden; auch Fingerabdrücke, Iris-Scans und Co. dürften demnach nicht ohne Erlaubnis gesammelt werden. Unternehmen, die sich daran nicht halten, können beklagt werden. Des Weiteren muss Clearview sein kostenloses Testprogramm für Polizeibeamte beenden und ein Opt-Out-Verfahren anbieten und dieses für 50.000 US-Dollar bei Google, Facebook oder in anderen Medien bewerben.

Nathan Freed Wessler, stellvertretender Direktor des ACLU Speech, Privacy, and Technology Projects, kommentierte: „Indem Clearview aufgefordert wird das […] biometrische Datenschutzgesetz von Illinois […] im ganzen Land einzuhalten, zeigt diese Einigung, dass strenge Datenschutzgesetze einen echten Schutz vor Missbrauch bieten können. Clearview kann die eindeutigen biometrischen Identifikatoren der Menschen nicht mehr als uneingeschränkte Gewinnquelle behandeln. […] andere Staaten sollten dem Beispiel von Illinois folgen und strenge biometrische Datenschutzgesetze erlassen.“

Für das Unternehmen stelle die Entscheidung keine wesentliche Änderung des Geschäftsmodells dar, so Hoan Ton-That, CEO von Clearview: „Clearview AI erbringt seine Dienstleistungen derzeit nicht für Strafverfolgungsbehörden in Illinois, obwohl es dies rechtmäßig tun kann. Um einen langwierigen, kostspieligen und ablenkenden Rechtsstreit mit der ACLU und anderen zu vermeiden, hat sich Clearview AI bereit erklärt seine Dienstleistungen für einen bestimmten Zeitraum weiterhin nicht für Strafverfolgungsbehörden in Illinois anzubieten.“ Seine Haltung bezüglich Verkäufe an private Unternehmen wolle das Unternehmen nicht ändern. „Unsere Datenbank wird nur Regierungsbehörden zum Zwecke der Aufklärung von Straftaten zur Verfügung gestellt.“

Anwalt Lee Wolosky, der das Unternehmen vertritt, ergänzte: „Clearview AI wird keine Änderungen an seinem derzeitigen Geschäftsmodell vornehmen. Es wird sein Geschäftsangebot in Übereinstimmung mit geltendem Recht weiter ausbauen.“ Das Unternehmen werde die Anwaltskosten zahlen, die weitaus geringer seien als die Kosten für die Fortführung des Prozesses. Für

das im Rahmen der Einigung beschlossene Opt-Out-Verfahren muss Clearview ein öffentlich und online zugängliches Antragsformular zur Verfügung stellen. Dort können Einwohner von Illinois ein Foto hochladen und ein Formular ausfüllen, das es dem Unternehmen untersagt das Bild für andere Zwecke als das Opt-out-Verfahren zu verwenden. In den nächsten fünf Jahren wird Clearview dann versuchen die entsprechenden Bilder aus seiner Datenbank herauszufiltern (s.o. S. 124; Koch, Clearview: Umstrittene Gesichtserkennungs-App für private US-Firmen verboten, www.heise.de 10.05.2022, Kurzlink: https://heise.de/-7080199).

USA

Meta entschädigt wegen unzulässiger Gesichtserkennung

Meta entschädigt Nutzerinnen und Nutzer im US-Staat Illinois dafür, dass von Facebook ohne deren Zustimmung Gesichtserkennung eingesetzt wurde. 2015 hatten die Betroffenen eine Sammelklage gegen Meta, damals noch Facebook, eingereicht. Grund war Facebooks Praxis Nutzerfotos zu speichern und automatisch zu analysieren, um gegebenenfalls Personen darauf zu markieren. Der Biometric Information Privacy Act im US-Bundesstaat Illinois besagt, dass die automatische Gesichtserkennung nur nach einer expliziten Einwilligung des Nutzers eingesetzt werden darf.

Anfang 2021 hatten sich die Streitparteien auf einen Vergleich geeinigt: Meta sollte insgesamt 650 Millionen US-Dollar an die Betroffenen zahlen. Da sich rund 1,6 Millionen Facebook-Nutzerinnen und -Nutzer aus Illinois an der Sammelklage beteiligten, erhalten sie alle nun jeweils 397 US-Dollar. Die meisten bekommen das Geld offenbar per PayPal. Wer keine digitale Zahlungsmöglichkeit angegeben hat, soll einen unauffälligen braunen Umschlag mit einem Scheck bekommen (Friedrich, Unerlaubte Gesichtserkennung in Facebook: Meta entschädigt Nutzer in Illinois, www.heise.de 01.06.2022, Kurzlink: https://heise.de/-7129020).

USA

Fruchtbarkeitsarzt als Samenspender enttarnt

Nach Komplikationen bei ihrer ersten Schwangerschaft hat eine Frau, Arianna Huhn, sich für eine klinische Studie angemeldet, bei der sie die DNA-Proben von sich und ihren Eltern einreichen musste. Im weiteren Verlauf förderte dies einen Fall von Fruchtbarkeitsbetrug zu Tage: In den 70er-Jahren hatten sich Huhns Eltern für eine künstliche Befruchtung entschieden, bei der das Sperma ihres Vaters mit weiterem gemischt wurde. Der Arzt hatte empfohlen, die künstliche Befruchtung vor dem Kind geheim zu halten. Arianna Huhn fand nun heraus, dass es sich um das Sperma des Arztes handelte, das die Eizelle ihrer Mutter befruchtete.

Als ihre Eltern ihr anlässlich der Studie sagten, dass ihr Vater nicht ihr biologischer Vater war, begann Huhn nach ihrem genetischen Hintergrund zu forschen. Sie machte einen DNA-Test über ein Testkit bei AncestryDNA und untersuchte akribisch alle Übereinstimmungen der Ergebnisse. Um die Freundesliste ihrer neuen Kontakte ebenfalls zu durchsuchen, nutzte sie auch Facebook. Ihre Suche führte sie auch zu dem Mann, der ihre Mutter befruchtet hatte. Dieser gab am Telefon jedoch an eine Vasektomie, also eine Sterilisation, durchgeführt zu haben. Doch erneut fand das Herkunftsanalyse-Unternehmen eine Übereinstimmung – ihre genetische Tante, die Schwester des Arztes.

Nach erneuter Konfrontation entschuldigte sich der Arzt den Betrug nicht vorher zugegeben zu haben. Sein eigenes Sperma hatte er sonst seinem Kollegen für seine Patientinnen gespendet, während er das Sperma seines Kollegen für seine eigenen Patientinnen verwendete. Ihre Mutter sei allerdings die einzige, bei der er sein eigenes Sperma verwendet habe. Außerdem waren sich ihre Mutter und er auch außerhalb des Arzt-Patienten-Verhältnisses bekannt, weshalb Huhn wohl auch keine rechtlichen Schritte einleitete. Um das Erlebte zu verarbeiten, trat sie der Facebook-Gruppe „Donor Deceived“ mit inzwischen 113 Mitgliedern bei – einer Gruppe, in der Opfer von Fruchtbarkeitsbetrug sich austauschen.

In den USA gibt es auf Bundesebene und zumeist auch auf Ebene der Bundesstaaten keine Gesetze gegen Fruchtbarkeitsbetrug. Reproduktionsmedizin ist weitgehend unreguliert. Da immer mehr Menschen auf Ahnenkunde spezialisierte Dienste in Anspruch nehmen, werden Fruchtbarkeitsbetrügereien immer wieder entdeckt. Spenderanonymität wird in Zeiten massentauglicher DNA-Testkits von 23andMe und AncestryDNA für den Hausgebrauch in der Praxis immer mehr in Frage gestellt. 2020 berichteten Medien über einen Arzt, der 40 Jahre lang Patientinnen mit seinem Samen befruchtete. Im Jahr 2019 gab es einen Bericht über einen niederländischen Arzt, der auf diese Art und Weise schätzungsweise 200 Kinder gezeugt haben soll. In Deutschland darf ein Spender nicht mehr als 15 Kinder zeugen, in Großbritannien sind es bis zu 10 Familien. In einer Fruchtbarkeitsklinik in Los Angeles (Kalifornien) war es zu einem Fall von Embryonenverwechslung gekommen (Koch, Online-DNA-Test überführt Fruchtbarkeitsarzt, www.heise.de 19.06.2022, Kurzlink: https://heise.de/-7145126).

USA

Bürgerrechtsorganisationen fürchten Frauenkontrolle nach Abtreibungs-Urteil

Nachdem am 24.06.2022 in den USA das Oberste Gericht, der Supreme Court, das nationalweit geltende, auf den Fall „Roe vs. Wade“ zurückgehende liberale Abtreibungsrecht aufgehoben hat, könnten nach Befürchtungen von Bürgerrechtlern für Frauen, die abgetrieben haben, Datenspuren zum Verhängnis werden. Der mehrheitlich konservativ besetzte Gerichtshof machte mit dem Urteil den Weg für strengere Abtreibungsgesetze in den Bundesstaaten frei, bis hin zu kompletten Verboten. Einige US-Bundesstaaten hatten sich durch „trigger laws“ schon auf die Entscheidung vorbereitet, in Staaten wie Arkansas, Kentucky oder Louisiana sind Abtreibungen nun nicht mehr erlaubt. Ausnahmen gibt es in der Regel nur für

medizinische Notfälle. Es wird erwartet, dass die Hälfte der Bundesstaaten Abtreibungen verbietet.

So könnten beispielsweise Apps für Frauen, mit denen diese ihren Zyklus verfolgen, zum Verhängnis werden, wenn damit erfasste Daten künftig in Strafverfahren als Beweismittel herangezogen werden. Die Nicht-Regierungsorganisation (NGO) Center for Democracy and Technology (CDT) erklärte: „Im digitalen Zeitalter öffnet diese Entscheidung die Tür für Strafverfolgungsbehörden und private Kopfgeldjäger, die riesige Mengen an privaten Daten von gewöhnlichen Amerikanern suchen". Daten, die sensible Informationen zum Menstruationszyklus aufzeigen, könnten von Datenbrokern ohne Wissen der Benutzer gesammelt und verkauft werden. Datenquellen könnten auch Webbrowser- und Suchverläufe sein, E-Mails oder SMS. CDT meint, dass nach der Entscheidung des Supreme Court Technologieunternehmen verstärkt die digitale Privatsphäre der Frauen schützen müssten. Sie könnten die Ende-zu-Ende-Verschlüsselung ausweiten und weniger Daten sammeln und weiterverkaufen, die zeigen können, ob eine Frau schwanger ist. Ebenso bedenklich schätzen die Bürgerrechtler Techniken mit „künstlicher Intelligenz" ein, die solche Daten preisgeben könnten. Vor allem müssten diese Unternehmen Anträge von Strafverfolgern genau prüfen, die dem Verdacht einer verbotenen Abtreibung nachgehen und Daten herausgegeben haben wollen. Die Nutzerinnen sollten rechtzeitig über solche Anfragen informiert werden und die Öffentlichkeit über die gesamte Anzahl von Anforderungen von Strafverfolgungsbehörden.

Und die NGO Electronic Frontier Foundation (EFF) warnte: „Alle Menschen, die eine Möglichkeit für eine Abtreibung suchen, anbieten oder erleichtern, müssen jetzt davon ausgehen, dass alle Daten, die sie online oder offline zur Verfügung stellen, von den Strafverfolgungsbehörden gesucht werden könnten." Nutzer sollten die Datenschutzeinstellungen für die von ihnen verwendeten Dienste sorgfältig überprüfen, Ortungsdienste, die sie nicht benötigen, in Apps deaktivieren und verschlüsselte Messaging-Dienste verwenden.

Die Bürgerrechtler von Fight for the Future fordern die US-Regierung und das Parlament auf die Überwachung durch Unternehmen, deren Datensammelei und Vorratsdatenspeicherung zu beenden. Nach der Entscheidung des Supreme Court zeige sich umso mehr, dass der Überwachungskapitalismus als Geschäftsmodell mit grundlegenden Menschenrechten unvereinbar sei. Dessen Techniken eigneten sich perfekt, um Frauen zu verfolgen, die abtreiben wollen oder abgetrieben haben. Fight for the Future weist darauf hin, dass nicht nur Gesundheitsdaten für Frauen heikel sein können. Zusammen mit Amnesty International und anderen Organisationen hatten die Bürgerrechtler bereits früher von Google gefordert unnötige Handy-Standortdaten nicht mehr zu erfassen. Durch Standortdaten könnte Frauen beispielsweise nachgewiesen werden, dass sie eine Abtreibungsklinik aufgesucht haben (s.u.).

Mobiltelefondaten können als „Fenster zur Seele" missbraucht werden und Auskunft geben über eine Schwangerschaft und ein Schwangerschaftsende. Die Befürchtung, dass Daten aus Zyklus-Apps nicht sicher gespeichert sind, wurde im September 2021 genährt: Frauen, die die beliebte App Flo nutzen, haben den Anbieter verklagt, weil er Daten an Google, Facebook, AppsFlyer und Flurry weitergegeben haben soll. Gemäß Cory Doctorov von der Electronic Frontier Foundation (EFF) sollten sich Frauen nicht der Illusion hingeben, das Löschen einer Zyklus-App würde ihnen Sicherheit geben. Das Problem liege grundsätzlicher, nämlich bei allen Apps, die etwa über Google oder Facebook verbreitet werden – von solchen für Distanzunterricht bis zu jenen, mit denen Muslime an ihre Gebete erinnert werden.

Einige Unternehmen in den USA hatten bereits vor der Entscheidung des Supreme Court angekündigt ihren Mitarbeiterinnen Schwangerschaftsabbrüche zu erleichtern, darunter auch Amazon. Meta hatte es seinen Mitarbeitern kurz nach dem Urteil untersagt im internen Netz darüber zu diskutieren. Die American Civil Liberties Union (ACLU) befürchtet, dass die Entscheidung und damit verbundene Haltung des Supreme Courts sich auch auf andere Bereiche auswirken könne wie zum Beispiel die gleichgeschlechtliche Ehe und die Empfängnisverhütung (Wilkens, US-Bürgerrechtler sorgen sich nach Urteil zur Abtreibung um den Datenschutz, www.heise.de 27.06.2022, Kurzlink: https://heise.de/-7154534; Brühl, Was Smartphones über Abtreibungen verraten können, SZ 06.07.2022, 22).

USA

Schwangerschaftsabbruch-Suche über Google riskant

Gemäß einer Studie des gemeinnützigen Center for Countering Digital Hate liefern die Ergebnisse von Google-Suchen nach „Abtreibung" genau das Gegenteil: Zentren von Abtreibungsgegnern. In einem Brief fordern US-Gesetzgeber Google nun auf genauere Ergebnisse zu liefern. Der Studie zufolge lieferten 11% der angezeigten Ergebnisse in der Google-Suche nach „Abtreibungsklinik in meiner Nähe" oder „Abtreibungspille" statt Kliniken, die Schwangerschaftsabbrüche vornehmen, sogenannte „Krisenschwangerschaftszentren", die Frauen von einem Schwangerschaftsabbruch abhalten wollen. Der Brief, der Google zur Ausgabe von genaueren Ergebnissen auffordert, wurde am 17.06.2022 aufgrund der Studie an Google gesendet und von 14 Senatoren und 7 Mitgliedern des US-Repräsentantenhauses unterzeichnet – alle Demokraten. Google solle keine Anti-Abtreibungskliniken oder „Fake-Krisenschwangerschaftszentren" in den Suchergebnissen anzeigen oder aber mindestens „angemessen kennzeichnen". In der Vergangenheit hätten die Frauen in diesen Einrichtungen ungenaue Informationen zu ihrer Schwangerschaft bekommen. Das könne den Zugang zu einer Abtreibung gefährden.

Google lehnte einen Kommentar direkt zu dem Brief, der direkt an CEO Sundar Pichai adressiert war, ab und erklärte: „Wir suchen immer nach Möglichkeiten unsere Ergebnisse zu verbessern und den Menschen zu helfen das zu finden, wonach sie suchen, oder zu verstehen, dass das, was sie suchen, möglicherweise nicht verfügbar ist."

Die Studie wurde in 13 US-Bundesstaaten durchgeführt, die nach der Entscheidung des Obersten Gerichtshofs der USA über die Anfechtung des Urteils „Roe vs. Wade" den Schwangerschaftsabbruch verbieten oder dies planen. Dabei kam auch heraus, dass in den Staaten 28% der Google-Anzeigen Anti-Abtreibungs-Zentren beinhalten würden, ebenso wie 37% der Ergebnisse auf Google Maps.

Im Mai 2022 war bekannt geworden, dass eine US-Firma auf Smartphones gesammelte Standortdaten zu An- und Abreise zu Einrichtungen verkauften, die unter anderem auch Abtreibungen durchführen. Auch Körperkameras und Nummernschildverfolgung werden bereits eingesetzt, um Menschen nachzuspüren, die zu Abtreibungskliniken kommen. Das Thema Abtreibung spaltet die USA und seine Bürger (Mewes, Schwangerschaftsabbruch: Google schickt Frauen teilweise zu Abtreibungsgegnern, www.heise.de 19.06.2022, Kurzlink: https://heise.de/-7145102).

USA

T-Mobile nach Datenleak zu Vergleich über 500 Mio. US-Dollar bereit

Die US-amerikanische Telekom-Tochterfirma T-Mobile US will mit einer Zahlung von einer halben Milliarde Dollar Nutzerklagen nach einem großen Cyberangriff beilegen. Davon sollen 350 Mio. US-Dollar (343 Mio. Euro) in einen Fonds für klagende US-Kunden fließen. Weitere 150 Mio. Dollar will T-Mobile US demnach in diesem und im kommenden Jahr für die Verbesserung der Cybersicherheit ausgeben.

T-Mobile US hatte im August 2021 bestätigt, dass Daten von Millionen Kunden gestohlen wurden (DANA 4/2021, 258). Laut Gerichtsunterlagen sind davon 76,6 Mio. US-Einwohner betroffen. Zu den erbeuteten Nutzerdaten gehörten unter anderem Namen und Telefonnummern. Etwas später wurde bekannt, dass die unbekannten Angreifer eine Lücke in einem ungeschützten Router genutzt hatten. Dafür hätten sie die Internetadresse von T-Mobile mit einem öffentlich zugänglichen Tool nach Schwachstellen abgesucht.

Nach dem Cyberangriff wurde T-Mobile US in Sammelklagen unzureichender Schutz der Nutzerdaten vorgeworfen. Im Dezember 2021 wurden in Missouri mehrere Klagen gebündelt (Case No. 21-md-03019-BCW). Wie in solchen Fällen üblich, hält T-Mobile US ausdrücklich fest, dass die Vereinbarung kein Schuldeingeständnis bedeute. Dem Deal muss noch der zuständige Richter im US-Bundesstaat Missouri zustimmen. Das kann nach Einschätzung von T-Mobile US im Dezember passieren – Berufungsverfahren könnten aber noch für Verzögerungen sorgen, hieß es.

T-Mobile US hatte nach eigenen Angaben zum Ende des ersten Quartals 2022 in den USA knapp 110 Mio. Kundinnen und Kunden. Mit ihnen setzte das Unternehmen in den drei Monaten 20 Milliarden US-Dollar um und erwirtschaftete einen Nettogewinn von 713 Mio. US-Dollar. Im April 2022 erhöhte die Deutsche Telekom ihre Beteiligung an der US-Tochter auf 48,4% (Wilkens, Datenklau: T-Mobile US will 500 Millionen Dollar im Vergleich zahlen, www.heise.de 24.07.2022, Kurzlink: https://heise.de/-7188520).

USA/China

Videoüberwacher Hikvision im Visier der US-Administration

Die chinesische Firma Hikvision stand bisher nicht im öffentlichen Rampenlicht, ist aber mit ihren Überwachungssystemen für die Polizei bis hin zu Babyfonen in mehr als 190 Ländern präsent. Die Fähigkeit, qualitativ hochwertige Produkte zu günstigen Preisen herzustellen und gute Drähte zum chinesischen Staat haben dazu geführt, dass Hikvision zum größten Hersteller von Videoüberwachungstechnik weltweit geworden ist. Das Unternehmen hat Chinas massives polizeiliches Überwachungssystem mit aufgebaut und es auf die Unterdrückung der muslimischen Minderheit in Xinjiang zugeschnitten. Deshalb hat die US-Regierung seit 2019 mehrmals Sanktionen gegen das Unternehmen verhängt.

• SDN-Sanktion geplant

Noch im Jahr 2022 erwägt das US-Finanzministerium offenbar Hikvision in die Liste der „Specially Designated Nationals and Blocked Persons" (SDN) aufzunehmen, die normalerweise Pariastaaten wie Nordkorea oder dem Iran vorbehalten ist. Die Aufnahme in die SDN-Liste würde aus US-Prespektive quasi jedem weltweit verbieten mit Hikvision Geschäfte zu machen. Dies wäre eine härtere Sanktion als die, der beispielsweise das chinesische Unternehmen Huawei unterliegt. Denn Länder und Unternehmen würden riskieren auf dieselbe Liste der USA gesetzt zu werden, wenn sie sich nicht daran halten. Die Millionen von Hikvision-Kameras, die derzeit im Einsatz sind, müssen zwar nicht über Nacht entfernt werden, doch sie würden in Zukunft nicht mehr zum Verkauf angeboten. Conor Healy, der bei IPVM, einer Online-Fachpublikation für die Videoüberwachungsbranche, zu Hikvision recherchiert hat, erklärte: „Dadurch könnte Hikvision sehr schnell zu einem rein einheimischen Unternehmen werden."

• Eine globale Erfolgsgeschichte

Hikvision wurde 2001 gegründet und war perfekt positioniert, um aus den Sicherheitsverschärfungen in vielen Ländern nach den Anschlägen am 11.09.2001 Kapital zu schlagen. Das Unternehmen begann mit dem Verkauf von Capture-Karten, die in Überwachungssystemen verwendet werden und Videosignale digitalisieren. 2007 führte das Unternehmen seine eigenen Kameras ein. Heute verkauft das Unternehmen alles, von der Software bis zur Hardware – in der Regel zu wesentlich günstigeren Preisen als die internationale Konkurrenz.

Das Gründungsteam bestand hauptsächlich aus Ingenieuren der China Electronics Technology Group Corporation (CETC), einem staatlichen Unternehmen, das elektronische Produkte für zivile und militärische Zwecke herstellt. Im Jahr 2008 übertrug Hikvision 48% seiner Anteile an CETC, wodurch Hikvision offiziell zur Tochtergesellschaft eines staatlichen Unternehmens wurde.

Wie in vielen Ländern ist auch in China die Regierung der größte Überwachungskunde. Mit Hilfe seines staatlichen Hintergrunds erhielt Hikvision schon bald große und kleine Aufträge von lokalen Regierungen zum Bau von Polizeiüberwachungs- oder Verkehrskontrollsystemen. Vor allem wurde Hikvision zu einem wichtigen Bestandteil der chinesischen Polizeiprojekte „Skynet" und „Sharp Eyes", die darauf abzielen in jeder Straße Kameras zur Überwachung der Menschen aufzustellen. 2018 erhielt Hikvision einen 125-Millionen-US-Dollar-Auftrag für den Bau und die Aktualisierung von 45.000 Kameras in der chinesischen Stadt Xi'an, von denen 16.000 Stück mit Funktionen zur Menschen- oder Gesichtserkennung ausgestattet werden sollen.

Hikvision war von Anfang an global ausgerichtet. 2004 begann das Unternehmen seinen Namen in mehr als hundert Ländern als Marke registrieren zu lassen. 2010 war das Unternehmen dank seines Netzwerks von Überwachungskameras, die über Digital-Video-Recorder-Systeme (DVR) ihre Daten speichern, der weltweit führende Anbieter von digitalen Videoaufzeichnern. Die Verkäufe in Übersee machten 27% des Umsatzes von 12,42 Mrd. US-Dollar im Jahr 2021 aus.

Eine Studie des Branchenmediums Top10VPN aus dem Jahr 2021 nutzte die Shodan-Suchmaschine (die das Internet nach den eindeutigen IP-Adressen von Geräten, in diesem Fall Kameras, durchsucht) und fand 4,8 Millionen Netzwerke mit Hikvision-Geräten in 191 Ländern außerhalb Chinas. Mit über 600.000 Hikvision-Systemen haben die USA die zweithöchste Anzahl an Kameras des Unternehmens, gleich nach Vietnam. Jedes dieser gefundenen IP-Netzwerke kann bis zu 24 Hikvision-Kameras unterstützen.

Allein in London wurden 55.455 Hikvision-Netzwerke gefunden. Samuel Woodhams, Researcher bei Top10VPN, der die Studie durchgeführt hat, meinte: „Nach meiner Erfahrung, die ich bei einem Spaziergang durch London gewonnen habe, liegt die Zahl wahrscheinlich um ein Vielfaches höher. Sie sind in fast jedem Supermarkt zu finden." Die weite Verbreitung von Hikvision-Kameras im Ausland hat Ängste um die nationale Sicherheit ausgelöst, auch wenn nicht bewiesen ist, dass das Unternehmen seine Daten aus dem Ausland zurück nach China überträgt. 2019 verabschiedeten die USA ein Gesetz, das Hikvision jegliche Verträge mit der dortigen Bundesregierung verbietet.

• Repressionskomplize der chinesischen Regierung

Berüchtigt wurde Hikvision durch seine Beteiligung an Chinas Unterdrückungssystem in Xinjiang gegen die dortige muslimische Minderheit der Uiguren. Zahlreiche Überwachungskameras, von denen viele mit fortschrittlicher Gesichtserkennung ausgestattet sind, wurden sowohl innerhalb als auch außerhalb von Umerziehungslagern in Xinjiang installiert, um die Kontrolle der Regierung über die Region zu stärken. Und Hikvision hat einen großen Anteil an den Aktivitäten. Es wurde festgestellt, dass das Unternehmen mindestens 275 Mio. US-Dollar an Regierungsverträgen zum Aufbau von Überwachungsanlagen in der Region erhalten hat und KI-Kameras entwickelt wurden, die physische Merkmale uigurischer Ethnizität erkennen können.

Auf von MIT Technology Review gestellte Fragen zu Xinjiang antwortete Hikvision mit der allgemeinen Erklärung, dass das Unternehmen „die geltenden Gesetze und Vorschriften in den Ländern, in denen wir tätig sind, strikt befolgt" und weiterhin befolgen werde „und dabei eine international anerkannte geschäftliche Ethik" sowie lokale Geschäftsstandards beachte. Darren Byler, Anthropologe an der Simon Fraser University und Autor von „In the Camps: Chinas High-Tech-Strafkolonie", meinte dazu: „Die Art und Weise, wie [Unternehmen wie Hikvision] in der Lage sind Menschen durch Kontrollpunkte und Gesichtserkennungssysteme in ihrer Freiheit zu beschränken, hat die gesamte Region, zumindest aus Sicht der Uiguren, in ein scheinbar flexibles aber nach außen geschlossenes System verwandelt. Sie sprechen oft von einem Freiluftgefängnis. Und das wäre ohne diese Technologieunternehmen wirklich nicht möglich."

• Drohende Konsequenzen

Die Aufnahme von Hikvision auf die SDN-Liste würde die Spannungen zwischen den USA und China verschärfen. Nach einer solchen Entscheidung, so Healy, könnten Personen strafrechtlich verfolgt werden, die mit dem Unternehmen arbeiten oder Geschäfte machen: „[Hikvision] kann nicht mehr mit dem US-Dollar oder dem US-Finanzsystem interagieren. Und andere Banken und andere Finanzinstitute in der ganzen Welt werden im Allgemeinen auch keine Geschäfte mit ihnen machen, weil sie ihren Zugang zum US-Dollar und zu den US-Finanzmärkten aufrechterhalten wollen." Welche Konsequenzen die Aufnahme auf die SDN-Liste konkret für Hikvision bedeuten würde, ist noch unklar. Die herkömmlichen Sanktionsinstrumente waren bisher nicht für das Internet konzipiert. Jon Bateman, Senior Fellow für Technologie und internationale Angelegenheiten beim Carnegie Endowment for International Peace meinte: „Wir befinden uns in einer Ära der Schaffung von Präzedenzfällen in Bezug auf restriktive Maßnahmen."

Bisher wurde kein großes Technologieunternehmen, dessen Produkte weltweit verkauft werden, auf die SDN-Liste gesetzt. Huawei, das derzeitige „Aushängeschild" für Technologieunternehmen im Spannungsfeld zwischen den USA und China, darf keine US-Produkte kaufen, keine US-Investitionen erhalten oder in den USA Geräte verkaufen, aber Huawei-Produkte werden weiterhin außerhalb der USA verkauft. Sollte Hikvision tatsächlich auf der SDN-Liste landen, wäre dies ein Experiment mit der Frage, wie Technik – sowohl Hardware als auch Software – international verboten werden kann.

Berichten der Financial Times zufolge informieren US-Diplomaten bereits ausländische Regierungen darüber, was die USA mit Hikvision zu tun gedenken. Die härteren Sanktionen werden wahrscheinlich in Ländern wie Großbritannien oder Norwegen begrüßt, die ihre eigenen Untersuchungen über die Mitschuld von Hikvision an Menschenrechtsverletzungen in Xinjiang durchgeführt haben. Bateman warnt jedoch davor, dass – da die Sanktionen in erster Linie eine einseitige Entscheidung der USA sind – nicht jedes andere Land zwangsläufig mit der Strenge und dem Ausmaß der Maßnahmen einverstanden sein wird: „Je mehr die US-

Regierung von diesen unilateralen Instrumenten Gebrauch macht, desto mehr Fragen werden in den ausländischen Hauptstädten aufgeworfen, ob sie bei der Anwendung dieser Instrumente ein Mitspracherecht haben, und wenn ja, in welchem Umfang."

China hat seinerseits seine Unterstützung für Hikvision zum Ausdruck gebracht. Als Reaktion auf die Nachricht über die möglichen Sanktionen beschuldigte ein Sprecher des Außenministeriums die USA „die staatliche Macht und das nationale Recht zu missbrauchen, um chinesische Unternehmen mutwillig zu unterdrücken". Der florierende Inlandsmarkt in China mag Hikvision noch am Leben erhalten, doch für chinesische Unternehmen, die sich im Ausland einen Namen machen wollen, wäre dies ein großer Rückschlag (Yang, Videoüberwachung: Die größte Überwachungsfirma, von der Sie nie gehört haben, www.heise.de 12.07.2022; Kurzlink: https://heise.de/-7158966).

Technik-Nachrichten

Apple testet Gesichtserkennung illegal an Mitarbeitenden

Die 35-jährige ehemalige Apple-Projektmanagerin und Whistleblowerin Ashley Gjovik legte offen, dass der Apple-Konzern seine Mitarbeitenden und Fotos von deren Gesichtern in unzulässiger Weise als Material für das Training seiner Gesichtserkennungssoftware benutzte. Im August 2017 hatte sie eine E-Mail erhalten, in der sie zu einer „Data Collection Social Hour" eingeladen wurde. Auf der Datenparty sollte es Getränke und Musik sowie „20 Minuten Datensammlung in sozialer Umgebung" geben. Eingeladen waren nur festangestellte Beschäftigte. Solche, die empfindlich auf Licht reagierten, waren von dem Event ausgeschlossen. Eigentlich bestand keine Verpflichtung die Datenparty zu besuchen, so Gjovik. Für sie habe sich das Ganze aber nicht wirklich freiwillig angefühlt.

Die „Party" erwies sich als Zusammenkunft auf einem Parkplatz, umgeben von schwarz verkleideten drei Meter hohen Stahlzäunen und überwacht von Security und Kameras. An der Bar habe ein misslauniger Mitarbeiter im Hawaii-Hemd bedient; ein Anderer führte Gjovik und vier andere Apple-Beschäftigte an einen Klapptisch und erklärte den Anwesenden, dass sie Selfies aus allen Lagen machen sollten – mit einer eigens entwickelten App: Glimmer. Ziel war es die Algorithmen der Gesichtserkennungssoftware Face-ID von Apple zu trainieren.

Sie unterschrieb eine digitale Einverständniserklärung, von der sie nie eine Kopie bekam. Dann habe jeder das neue, noch nicht veröffentlichte iPhone-Modell X erhalten, auf dem „Gobbler" (auf deutsch „Verschlinger") installiert war. Später änderte Apple den Namen in „Glimmer". Bei knapp 40 Grad in der brütenden Sonne habe sie sich dann, so Gjovik, schwitzend selbst fotografiert, von oben, von der Seite, mit Sonnenbrille oder Grimasse schneidend. So sollten die Apple-Mitarbeiter den Algorithmus von FaceID füttern. Das Feature dient dazu das Mobilphone über Gesichtserkennung zu entsperren. Apple setzte, so Gjovik, neben solchen Datenpartys wohl auch auf heimlich geschossene Bilder seiner Angestellten aus intimen Situationen.

Um die Gesichtserkennung zu verbessern, soll Apple seinen Mitarbeitenden ein iPhone X auf dem sie – im Apple-Sprech – „leben" sollten, mit vorinstallierter Glimmer-App zur Verfügung gestellt haben und die Nutzer:innen über Jahre permanent und automatisch fotografiert haben. Mitarbeitende, die 100 Bilder pro Tag oder 2.000 Bilder im Monat von sich hochluden, erhielten einen virtuellen Orden. Zwangsläufig wurden dabei auch Bilder von Freunden, Geschwistern oder Wildfremden erfasst, die dem Ganzen nicht einmal formal zugestimmt hatten. Der Studienleiter hatte die Teilnehmenden instruiert: „Alle Daten, die eure Gesichter im Bild haben, sind gute Daten." Der Algorithmus sei „datenhungrig". Ende 2020 prahlte der Studienleiter in einem Blogbeitrag, Apple habe für den Start von FaceID eine Milliarde Bilder gesammelt. Rund vier Jahre lang fotografierte die App sie im Halbschlaf oder auf der Toilette; selbst Nacktbilder, so Gjovik, seien von ihr gespeichert gewesen. Sie schätzt, dass hunderte Bilder pro Tag von der App aufgenommen wurden. Zu einem Widerspruch habe sie sich zunächst nicht getraut: „Apples Kultur der Geheimnistuerei sickert tief ins Bewusstsein ein. Du hast Angst selbst mit Behörden über offensichtliches Fehlverhalten zu reden."

Im August 2021 löste Gjovik mit der Offenlegung dieser Praktiken einen Skandal im Apple-Universum aus und musste letztlich den Konzern verlassen. Nach Abschluss ihres Jurastudiums hat sich die ehemalige Apple-Mitarbeiterin im Juni 2022 wegen möglicher Verletzung ihrer Privatsphäre an die kalifornische Datenschutzbehörde sowie den Bundesdatenschutzbeauftragten in Deutschland gewandt. Der Fall liegt jetzt bei der bayerischen Datenschutzbehörde, weil sich Apples Deutschlandzentrale in München befindet. Dort forscht Apple auch an Bilderkennung und FaceID.

Weil Angestellte trotz Einwilligungserklärung durch das Abhängigkeitsverhältnis zu ihrem Arbeitgeber bei solchen fragwürdigen Aktionen nicht wirklich freiwillig mitgemacht haben könnten, sieht die Arbeitsrechtlerin Annegret Balzer durchaus die Möglichkeit eines Datenschutzverstoßes seitens Apple gegeben. Dann könnte dem iPhone-Konzern eine Strafe in Millionenhöhe drohen.

Im September 2021 feuerte Apple die Frau nach sechseinhalb Jahren im Unternehmen, weil sie mit der Veröffentlichung der Bilder ihre Vertraulichkeitsverpflichtung gebrochen habe, so Apple-Anwälte im März 2022 in einer Stellungnahme an das Whistleblowerprogramm des US-Arbeitsministeriums. Gjovik arbeitet inzwischen bei einer Nichtregierungsorganisation, die gegen Zensur in China kämpft. Sie wehrt sich vor dem US-Arbeitsschutzgremium NLRB gegen ihre Kündigung. Apple wiederum argumentiert mit der Verletzung einer Vertraulichkeitsvereinbarung durch die Whistleblowerin. Die Börsenaufsicht SEC interessiert sich für den Fall; sie möchte wissen, ob Apple eine Whistleblowerin kaltstellen will. Das Verfahren kann sich lange hinziehen. Statt eines iPhones nutzt Gjovik jetzt ein Android-Smartphone.

Die Aktion Apples ist von Interesse, da sich der Konzern in der Öffentlichkeit gern als Vorreiter in puncto Datenschutz präsentiert. Hinter den Kulissen scheint dafür aber wenig Platz zu sein. Apple-Chef Tim Cook stellt sich immer wieder als Vorreiter des Datenschutzes dar: „Wenn wir anfangen uns permanent überwacht zu fühlen, verändert sich unser Verhalten. Wir fangen an weniger zu tun, weniger nachzudenken." Die Maßnahmen des Konzerns etwa gegen das App-Tracking – die entsprechenden Einstellungsmöglichkeiten sollen allein Meta (Facebook) Milliarden kosten – können den Eindruck vermitteln, dass es der iPhone-Konzern mit dem Datenschutz durchaus ernst meint.

Dass der Einsatz von Glimmer heikel ist, scheint Apple durchaus bewusst zu sein. Im August 2017 schrieb der Leiter der Studie zur Gesichtserkennung in einer Mail an Teilnehmer, dass Mitarbeiter aus Frankreich und Deutschland ausgeschlossen seien. Eine solche Nutzerstudie, so später in einem LinkedIn-Post, würde nach der dortigen Rechtslage immer als Zwang interpretiert (Beuth/Demling, iPhone is watching you, Der Spiegel Nr. 26, 25.06.2022, 74 ff.; Brien, Whistleblowerin: Apple lud Mitarbeiter zu Datenparty, um Face-ID fürs iPhone zu trainieren, https://t3n.de/news/whistleblowerin-apple-datenparty-1481776/ 24.06.2022).

Vodafone drängt mit TrustPid auf den Werbemarkt

Bisher leiten Mobilfunkprovider den Datenverkehr ihrer Endkunden weitgehend unangetastet ins Internet weiter. Mit TrustPid würde Vodafone in diesen Datenverkehr eingreifen und den Nutzern eine feste Kennung zuweisen, die sich unter anderem nach der Mobilfunknummer eines Kunden richtet. Diese Kennung könnten dann Website-Betreiber abrufen, um genau zu erfassen, welche Inhalte sich ein Mobilfunknutzer anguckt, um daraus ein Personenprofil zu bilden und zielgerichtet Werbung auszuspielen. Das Argument: Nur über solche Datengeschäfte könnten viele Online-Angebote genug Einkünfte erwirtschaften, um in Zukunft kostenfrei zu bleiben.

Werbetreibende suchen nach entsprechenden Lösungen. Seit der iPhone-Hersteller Apple begonnen hat das allumfassende Tracking zu Werbezwecken zurückzudrängen, beklagen sich große Markenartikler, dass sie noch allenfalls die Hälfte der Werbe-Cookies verwenden können. Wenn Google 2023 wie geplant den Werbe-Cookie in Chrome abschaltet, müsste die technische Grundlage des Anzeigengeschäfts auf eine völlig neue technische Grundlage gestellt werden.

Die Werbebranche will sich aber auch künftig nicht auf unpersonalisierte Werbung beschränken und zum Beispiel Auto-Werbung bevorzugt bei Websites und Artikeln mit Autobezug ausspielen. Daher hat ein regelrechtes Wettrennen der Anbieter von Werbe-IDs begonnen, die ihrer Kundschaft versprechen Nutzer auch weiterhin tracken zu können. Einerseits versucht die Branche die Tracking-Sperren technisch zu umgehen. Dazu werden die Werbe-Cookies zum Beispiel auf unverdächtige Server verschoben. Oder die Nutzer werden beim Besuch einer Webseite im Hintergrund über verschiedene andere Domains umgeleitet, die dann selbst Cookies setzen. Gleichzeitig wollen immer mehr Anbieter die Nutzer dazu bringen sich dauerhaft einzuloggen und dabei sämtliche Datenverarbeitungen zu akzeptieren.

Mobilfunkprovider wie Vodafone und die Telekom sind in einer einmaligen Position. Selbst wenn der Browser routinemäßig Cookies löscht oder sogar die IP-Adresse wechselt, kann der Provider immer noch den Datenverkehr mit der jeweiligen Mobilfunknummer verknüpfen. Die Werbekunden wollen zwar keinen Zugriff auf Namen oder die echte Mobilfunknummer bekommen, sondern nur auf eine pseudonyme Kennung. Diese kann aber schnell wieder einem konkreten Nutzerprofil zugewiesen werden, etwa, wenn man bei einem Online-Shop einkauft oder sich bei einem E-Mail-Provider einloggt.

Eine neue Funktion von Apple könnte das Geschäft aber wieder zunichtemachen. Beim sogenannten „iCloud Privat-Relay" werden die Daten verschlüsselt über die Server Apples umgeleitet, die Provider haben so keinen Zugriff mehr. Vodafone und die Deutsche Telekom haben deshalb bereits bei der Europäischen Kommission Beschwerde eingelegt. Parallel haben die Provider eine gemeinsame Lobby-Kampagne begonnen, um zu erreichen, dass sie den Datenverkehr ihrer Endkunden selbst monetarisieren dürfen, um den Netzausbau zu finanzieren. Die für das Digitale zuständige EU-Kommissarin Margrethe Vestager zeigte sich offen gegenüber solchen Vorschlägen.

TrustPid befindet sich bisher in einem Test-Stadium. Ein Sprecher von Vodafone Deutschland erklärte, dass der Dienst Teil einer „technischen Lösung für digitale Werbung in Europa" sei, von der „Verbraucher, Werbetreibende und Verlage gleichermaßen profitieren könnten". Wie viele Kunden an dem Testbetrieb teilnehmen, verrät Vodafone nicht. Der Sprecher versichert aber, dass diese über die Datenverarbeitung informiert seien. TrustPid ist bisher offenbar noch nicht routinemäßig bei allen Kunden von Telekom und Vodafone in Deutschland im Einsatz.

Bislang scheint sich auch nur eine einzige Website an dem Verfahren zu beteiligen. Bild.de hat einen Verweis auf das neue Programm in seine Datenschutzbedingungen aufgenommen und bietet auch ein Widerrufsformular an, um der Nutzung der Mobilfunk-ID zu widersprechen. Wohin die Reise geht, wird deutlich, wenn man die rudimentäre Website von TrustPid aufruft: Vodafone will nicht nur die

Werbekennung bereitstellen, sondern auch verwalten, wer auf diese Kennung zugreifen kann. So ist auf der Website eine Funktion eingebaut, mit der die Mobilfunk-Kunden ihre Zustimmung zur Datenverarbeitung bei einzelnen Werbepartnern erteilen oder widerrufen können. Dies würde den Providern eine zentrale Rolle bei der Werbevermarktung verschaffen, die sie sich natürlich bezahlen lassen wollen.

Bereits 2012 hatte der US-Provider Verizon eine ganz ähnliche Technik eingesetzt, um die eigenen Nutzer zu tracken. Erst Jahre später wurden die sogenannten unlöschbaren „Super-Cookies" bekannt und der Provider musste eine Geldstrafe zahlen. Solche Konflikte will Vodafone vermeiden und erklärte: „Wir nehmen den Schutz der Privatsphäre, Datensicherheit und die Einhaltung der Gesetze zum Datenschutz und zur Privatsphäre sehr ernst." Doch es ist fraglich, ob Nutzer überhaupt einschätzen können, wofür die Daten genutzt werden, die ihr Handy ständig über sie sammelt. Welches Ausmaß die Datensammelwut inzwischen erreicht, zeigt sich zum Beispiel in den USA, wo mehrere Daten-Broker routinemäßig mit den Profilen von Personen handelten, die eine Abtreibungsklinik besucht hatten (s.o. S. 195).

Selbst wenn die Mobilfunkprovider die Daten nicht direkt an solche Daten-Broker zuliefern, erleichtern Werbe-IDs wie von Vodafone die Verknüpfung verschiedener Datenquellen. Bisher nutzten Daten-Broker routinemäßig die Geräte-IDs von Apple und Google, was die Konzerne jedoch neuerdings bekämpfen.

Die Datenschutzbehörde in Nordrhein-Westfalen erklärte: „Aus unserer Sicht muss die Wirksamkeit der Einwilligung der Nutzer*innen hinterfragt werden." Die Datenverarbeitung für Nutzer müsse transparent gemacht und die Freiwilligkeit gewährleistet werden. Zudem sieht die Behörde Probleme darin, dass die persönlichen Daten nicht auf den Geräten der Nutzer, sondern auf externen Servern gespeichert werden. Die Behörde hat deshalb angekündigt, die Datenschutzkonformität von Trust-Pid genauer zu prüfen (Kleinz, Rückkehr der Super-Cookies, www.spiegel.de 28.05.2022).

TAB-Gutachten: Bargeld gewährleistet den besten Datenschutz

Das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) hat in einer Studie Veränderungen der klassischen Banken- und Bezahlsysteme sowie des damit einhergehenden Machtgefüges analysiert und warnt in seinem Resümee vor einer „Welt ohne Bargeld" und dem zunehmenden Einfluss von Big-Tech-Konzernen aus den USA und China auf das Finanzwesen. Damit werde sich künftig „stärker die Frage nach der Erhaltung der Handlungsfähigkeit des europäischen Bankenwesens stellen".

• Bargeld wichtiges Korrektiv

Die Forschenden vom Karlsruher Institut für Technologie (KIT), die zusammen mit Kooperationspartnern die TAB-Studie erstellt haben, betonen: „Gegenüber unbaren Zahlungsmitteln bildet Bargeld ein wichtiges Korrektiv im Zahlungsverkehr." Keine Debit- oder Kreditkarte und schon gar nicht Bitcoin und andere virtuelle Münzen erreichten „ein ähnlich hohes Inklusionsniveau" und einen ähnlich guten Schutz der Privatsphäre. „Trotzdem nimmt die Nutzung unbarer Zahlungsmittel auch in Deutschland weiter zu." Der Rückgang der Bargeldnutzung um 14% zwischen 2017 und 2020 auf 60% sei beträchtlich. Dieser könne aber „im Wesentlichen durch pandemieinduzierte Nachholeffekte bewirkt worden sein". Das Minus werde sich voraussichtlich in den nächsten Jahren wieder auf die üblichen ein Prozent pro Jahr einpendeln.

Die kartengestützten Zahlverfahren erfolgen entweder direkt mit der Debit- oder Kreditkarte am physischen Verkaufspunkt oder mit einer virtuellen Lösung beim mobilen Bezahlen und bei Internetlösungen, „über die unbare Zahlweisen im Hintergrund abgewickelt werden". Treiber seien neben der Corona-Pandemie etwa Preis, Verfügbarkeit und Verbreitung von Basistechnologien, Verbraucherwünsche und innovative Bezahlansätze. Vorteile unbarer Zahlungslösungen sehen die Autoren bei deren Einsetzbarkeit im E-Commerce sowie im grenzüberschreitenden Zahlungsverkehr und bei Schutzmechanismen.

• Datenschutz beim ePayment

Das Sicherheits- und Datenschutzniveau der jeweiligen Ansätze sei sehr unterschiedlich. So könne das Bezahlen mit Debitkarten im Vergleich zu vielen anderen unbaren Zahlweisen als relativ sicher bewertet werden. Auch die Privatsphäre werde dabei nicht so stark ausgehöhlt. Kreditkarten schnitten in beiden Punkten schlechter ab. Die Verfasser arbeiten heraus, dass bei neueren Online-Varianten wie Paypal & Co. sowie mobilem Bezahlen der Datenschutz noch niedriger als bei Kartenzahlungen sei. Hier würden auch Informationen erhoben und verarbeitet werden, „die nicht in unmittelbarem Zusammenhang mit dem Bezahlvorgang stehen". Beim Mobile Payment kämen zusätzlich zu generellen Authentifizierungsmechanismen zumindest Token zum Einsatz, was Missbrauch etwas einschränke. Ein zusätzlicher Sicherheitsfaktor sei gegeben, wenn biometrische Merkmale zur Entsperrung des Smartphones notwendig seien. Die Kritik: „Bei manchen unbaren Bezahlverfahren wie Sofortüberweisung wird der Grundsatz systematischer IT-Sicherheit verletzt." Demnach sollten „für jeden Anmeldeprozess und Diensteanbieter neue Zugangsdaten verwendet werden", die für keinen anderen Service oder Dritte bekannt sind. Nach der zweiten EU-Zahlungsdiensterichtlinie (PSD2) sei dies zulässig.

Große Unternehmen mit etablierten Tech-Plattformen wie Alibaba, Amazon und Facebook sind laut der Untersuchung „inzwischen etablierte Akteure im Zahlungsverkehr". Ihre Motive für den Markteintritt und die verfolgten Geschäftsmodelle seien vielfältig. Sie reichten von der Datengewinnung für Werbezwecke über das Ziel, Kunden möglichst lang im eigenen Ökosystem zu halten, bis zum Einstreichen von Entgelten durch das Angebot einschlägiger Produkte. Da Bezahlen dabei „mehr und mehr zu einer integrierten Funktion wird, laufen Banken Gefahr zu Abwicklern im Hintergrund zu werden und damit ihre Sichtbarkeit beim Kunden zu verlieren".

Als zentrale Ideen der Notenbanken in der EU, um Big Tech Paroli zu bieten, haben die Forschenden etwa Initiativen für Produkte für unterschiedliche Zah-

lungssituationen unter einer europäischen Dachmarke ausgemacht, die auf Instant Payments beruhen. Angepeilt würden so Echtzeitüberweisungen, bei denen der Transfer von Geldbeträgen nur wenige Sekunden dauert. Auch ein europäisches Kartensystem sei geplant. Ob diese Vorhaben zeitnah verwirklicht werden könnten bleibe aber abzuwarten.

Beleuchtet werden in der Studie auch die Auswirkungen von Krypto-Vermögenswerten mit Zahlungsfunktion. Mit diesen ließen sich etwa schnelle und kostengünstige grenzüberschreitende Transaktionen abwickeln; bislang führten sie aber ein Nischendasein im Zahlungsverkehr. Nicht an den US-Dollar & Co. gekoppelte Kryptowährungen wie Bitcoin erfüllten derweil „durch ihre von Spekulationen verursachte Preisvolatilität nicht die Geldfunktion". Sie eigneten sich vor allem nicht zur Wertaufbewahrung. Aufgrund vieler ihrer wichtigen Eigenschaften würden sie ferner „häufig für kriminelle Zwecke" verwendet.

• Elektronisches Zentralbankgeld

Die vor allem von Facebook getriebene Aussicht auf eine weltweit verfügbare private digitale Währung hat laut der Studie bei vielen Zentralbanken dazu geführt Überlegungen zur Einführung eigener digitaler Zentralbankwährungen anzustellen oder bereits existierende Projekte hierzu beschleunigt voranzutreiben. Je nach Ausgestaltung einer solchen Central Bank Digital Currency (CBDC) rund um Anonymität, Datenschutz und Sicherheit könnten solche Ansätze „ähnlich wie Bargeld eine Korrektivfunktion mit Blick auf die Produktkonzeption privater Zahlungsdienstleister haben". Mit CBDC seien Zahlungsströme besser kontrollierbar. Geldwäsche- und Terrorismusbekämpfung würden damit erleichtert. In den Händen autoritärer Regime wie China könnten so aber auch Aktivitäten von Systemkritikern und gewöhnlicher Bürger leichter überwacht werden. China scheine im CBDC-Bereich generell die meisten Fortschritte gemacht zu haben. Mitte 2021 habe aber ferner die Europäische Zentralbank entschieden die Potenziale eines E-Euros genauer auszuloten. Allgemein wäre die Einführung von digitalem Zentralbankgeld „ein erheblicher Einschnitt in das gegenwärtige Geld- und Banksystem".

Die Wissenschaftler gehen davon aus, dass die Erfahrungen aus der Pandemie „die Neugier auf die Vielfalt unbarer Zahlungslösungen und der mit ihnen kombinierbaren Produkte und Dienstleistungen wachsen lässt". In Verbindung mit einer von deutschen Banken gestützten einheitlichen Zahlungslösung für sämtliche Kanäle, einem europäischen Kartensystem nach europäischen Datenschutzstandards und einem perspektivisch verfügbaren digitalen Euro als alternatives gesetzliches Zahlungsmittel könnte dies den Rückgang der Bargeldnutzung deutlich verschärfen.

Möglicherweise müsste dann von den 2030-ern an „über die Notwendigkeit gesetzlicher Standards für eine Grundversorgung mit Bargeld wie in Schweden" nachgedacht werden. Dort spielen Münzen und Scheine kaum noch eine Rolle. Als Reaktion darauf habe die Regierung in Stockholm nicht nur ihr Projekt zur E-Krone vorangetrieben, sondern auch ein Gesetz erlassen, mit dem das Niveau der Bargeldversorgung des Jahres 2017 wiederhergestellt und gewährleistet werden soll. Bei solchen Gegenmaßnahmen tut sich dem TAB zufolge vor allem die Frage nach den Kosten für eine Bereitstellung der Bargeldinfrastruktur inklusive Geldautomaten und deren Übernahme auf (Krempl, Bundestag: Gutachter warnen vor „Welt ohne Bargeld", www.heise.de 10.07.2022, Kurzlink: https://heise.de/-7167699).

Rechtsprechung

EuGH

Umsetzung der Kontrolle mit Passenger Name Records wird eingeschränkt

Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 21.06.2022 die EU-Richtlinie zum Speichern und Rastern von Flugpassagierdaten von 2016 aufrechterhalten, in ihrer Anwendbarkeit eingeschränkt und für die Umsetzung in den nationalen Vorschriften hohe Auflagen festgelegt (Az. C-817/19). Das Urteil geht auf eine Klage der Menschenrechtsorganisation Ligue des droits humains (LDH) vor dem belgischen Verfassungsgerichtshof zurück, der 2019 dem EuGH Rechtsfragen vorgelegt hatte.

Gemäß der Richtlinie können die sogenannten Passenger Name Records (PNR) grundsätzlich bis zu fünf Jahre lang gespeichert werden. Zu den PNR gehören 18 Merkmale jedes Fluggastes, einschließlich sensibler Informationen: Namen, Kontaktdaten, Geburtsdatum, Begleitpersonen, eventuelle Vielfliegernummern, Angaben zum Flug, die zum Kauf des Fluges verwendeten Zahlungsmittel, ein nicht näher definiertes Freitextfeld. Religionszugehörigkeit, ethnische Herkunft und Gesundheitsdaten werden nicht erfasst, so wie zuvor in einem entsprechenden EU-Kanada-Abkommen, das vom EuGH aufgehoben wurde (DANA 3/2017, 174 ff.). Hauptzweck der Verarbeitung ist die Verhütung bevorstehender Verbrechen, etwa des Terrorismus oder schwerer Kriminalität.

Der EuGH betont nun, dass die Achtung der Grundrechte eine Beschränkung der in der PNR-Richtlinie vorgesehenen Befugnisse zur Übermittlung, Verarbeitung und Speicherung von Fluggastdaten auf das „absolut notwendige" erfordert. Werde vom nationalen Gesetz keine „reale und aktuelle oder vorhersehbare terroristische Bedrohung eines Mitgliedstaats" gefordert, so sei das Gesetz nicht mit dem EU-Recht

vereinbar. Dies sei der Fall bei einer anlasslosen Übermittlung und Verarbeitung von Fluggastdaten etwa bei Flügen innerhalb der EU sowie bei Beförderungen mit anderen Mitteln wie per Bahn oder Schiff innerhalb der Gemeinschaft.

In dem Urteil stellen die Luxemburger Richter fest, dass die Prüfung der vom belgischen Verfassungsgerichtshof vorgelegten Fragen nichts ergeben hat, was die Gültigkeit der PNR-Richtlinie an sich berühren könnte. Die EU-Vorgaben legen sie damit so aus, dass sie mit der Grundrechte-Charta der Gemeinschaft vereinbar sind. Eine ganze Reihe ihrer Erwägungsgründe und Bestimmungen erfordere eine solche Interpretation. Der EuGH verzichtet also auf eine völlige Aufhebung der zugrundeliegenden Richtlinie und versucht eine grundrechtskonforme Auslegung. Dieses Vorgehen, das beim deutschen Bundesverfassungsgericht gang und gäbe ist, ist für den EuGH vergleichsweise neu.

Das Gericht weist darauf hin, dass die PNR-Richtlinie „mit fraglos schwerwiegenden Eingriffen“ in Grundrechte wie das auf Privatsphäre und Datenschutz verbunden ist. Sie ziele „auf die Schaffung eines Systems kontinuierlicher, nicht zielgerichteter und systematischer Überwachung ab“, das die „automatisierte Überprüfung personenbezogener Daten“ sämtlicher Flugreisender einschließe. Dies mache es erforderlich die vorgesehenen Kompetenzen in der nationalen Umsetzung eng auszulegen.

Zu den vorzusehenden Schranken führen die Richter unter anderem aus, dass „die Anwendung des durch die Richtlinie geschaffenen Systems auf terroristische Straftaten und auf schwere Kriminalität mit einem – zumindest mittelbaren – objektiven Zusammenhang mit der Beförderung von Fluggästen beschränkt werden“ müsse. Sie dürfe sich etwa nicht auf strafbare Handlungen erstrecken, die zwar das in den EU-Vorgaben vorgesehene Kriterium in Bezug auf den Schweregrad erfüllten, angesichts der Besonderheiten des nationalen Strafrechtssystems aber zur „gewöhnlichen Kriminalität“ gehörten.

Die etwaige Ausdehnung der Anwendung der Richtlinie auf alle oder einen Teil der EU-Flüge muss sich laut dem EuGH „auf das absolut Notwendige beschränken“. Nötig sei ferner eine Möglichkeit der wirksamen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle, deren Entscheidung bindend ist. Ohne reale, aktuelle oder vorhersehbare terroristische Bedrohung dürften nur EU-Flüge einbezogen werden, die z.B. auf Basis konkreter Gefahrenanhaltspunkte bestimmte Flugverbindungen, Reisemuster oder Flughäfen betreffen.

Für die automatisierte Vorabkontrolle von Flugpassagierdaten, mit der Personen ermittelt werden sollen, die vor ihrer Ankunft oder ihrem Abflug genauer überprüft werden müssen, dürfen nationale PNR-Zentralstellen wie die beim Bundeskriminalamt (BKA) diese Angaben gemäß dem Urteil nur mit Datenbanken für Personen oder Gegenstände abgleichen, nach denen gefahndet wird oder die Gegenstand einer Ausschreibung sind. Diese Informationssysteme müssen ferner frei von Diskriminierung sein und von den zuständigen Behörden im Kontext der Bekämpfung terroristischer Straftaten und schwerer Kriminalität im Zusammenhang mit Flugreisenden betrieben werden.

Die Zentralstelle darf der Entscheidung zufolge bei der Auslese zudem anhand im Voraus festgelegter Kriterien keine Technologien der Künstlichen Intelligenz (KI) in Form selbstlernender Systeme („machine learning“) heranziehen, die ohne menschliche Einwirkung und Kontrolle den Bewertungsprozess und insbesondere die genutzten Kriterien sowie deren Gewichtung ändern können. Die Ablehnung von KI wird damit begründet, dass dabei die Kriterien verändert werden, anhand derer nach verdächtigen Mustern gesucht wird. Das würde den Rechtsschutz der Betroffenen unterlaufen. Verdachtsbewertungen müssen also menschengemacht bleiben. Die genannten Merkmale seien so festzulegen, „dass sie speziell auf Personen abzielen, bei denen der begründete Verdacht einer Beteiligung an terroristischen Straftaten oder schwerer Kriminalität im Sinne dieser Richtlinie bestehen könnte“. Dabei müssten „belastende“ und „entlastende“ Gesichtspunkte berücksichtigt werden, um Diskriminierungen zu vermeiden.

Zwecks einer anlasslosen Speicherung muss sich diese auf verdächtige Flugrouten beschränken, also etwa auf die typischen Wege von Schleusern oder Drogenschmugglern. Angesichts der Fehlerquote, die solchen automatisierten PNR-Verarbeitungen innewohnt, und der erheblichen Zahl der bereits aufgetretenen „falsch positiven“ Ergebnisse, hänge die Eignung des durch die Richtlinie geschaffenen Systems zur Erreichung der verfolgten Ziele im Wesentlichen vom ordnungsgemäßen Ablauf der manuellen Überprüfung der im Rahmen der automatisierten Verarbeitungen erzielten Treffer ab. Dafür müssten die EU-Staaten klare und präzise Regeln mit Kriterien für eine objektive Kontrolle vorgeben. In Deutschland lag die Trefferquote für potenzielle Gefährder 2019 bei 0,082 Promille.

Nach Ankunft oder Abflug der betreffenden Person dürfen PNR laut dem EuGH nur aufgrund neuer einschlägiger Umstände und objektiver Anhaltspunkte zur Verfügung gestellt und überprüft werden.

Der EuGH verdeutlicht, dass Artikel 12 der Richtlinie nationalen Vorschriften entgegenstehe, „die eine allgemeine, unterschiedslos für alle Fluggäste geltende Speicherfrist“ der einschlägigen Daten von fünf Jahren vorsehen. Nach Ablauf des ursprünglichen sechsmonatigen Zeitraums, in dem PNR im Klartext personenbezogen aufbewahrt werden dürfen, müsse die Speicherung der Daten wiederum „auf das absolut Notwendige beschränkt“ werden. Reisen mit anderen Beförderungsmitteln etwa zu Bahnhöfen oder Seehäfen könnten prinzipiell zwar mit erfasst werden – aber nur bei einem akuten Terrorbezug.

Der belgische Verfassungsgerichtshof muss nun klären, inwieweit das nationale PNR-System mit den EuGH-Leitlinien konform geht. Die in Belgien klagende LDH rügte den sehr großen Umfang der Daten sowie den allgemeinen Charakter ihrer Erhebung, Übermittlung und Verarbeitung. Das umsetzende Gesetz schränke die Freizügigkeit ein, da mit ihm auch alle Flüge innerhalb der EU sowie etwa Bus- und Bahnreisen erfasst und so indirekt wieder Grenzkontrollen eingeführt würden.

Weitere Beschwerden gegen die PNR-Sammlung aus anderen Mitgliedsstaaten sind anhängig. In Deutschland klagten mehrere Personen 2019 mit Unterstützung der Gesellschaft für Freiheits-

rechte (GFF) vor nationalen Gerichten gegen den automatisierten Transfer von Fluggastdaten durch Airlines wie die Lufthansa an das BKA. Gemäß dem deutschen Fluggastdatengesetz vom Mai 2018 kann das BKA Abgleiche mit Inpol-Fahndungsdateien sowie dem Schengener Informationssystem (SIS) vornehmen. Das Amtsgericht Köln legte dem EuGH die Frage vor, ob die hiesige Himmels-Rasterfahndung mit dem EU-Recht vereinbar sei. Die Bundesregierung bezeichnete das Vorgehen 2020 als verhältnismäßig. Die Fluggastdatenzentrale im BKA verarbeitete im gleichen Jahr rund 105 Millionen Passagierdatensätze, während es 2019 noch etwa 78 Millionen waren.

GFF-Anwalt Bijan Moini, der deutsche Klagen vertritt, bezweifelt, dass mit den Beschränkungen des EuGH viel gewonnen ist. Auch wenn die Sammelei auf angebliche Verbrecherrouten beschränkt werde, bleibe es bei dem Grundproblem, dass nach verdächtigen Mustern in an sich unverdächtigen Daten gesucht wird: „Das wird nach wie vor zu vielen Falschverdächtigungen führen" (Krempl, EuGH: EU-Fluggastdatenspeicherung rechtens, nationale Umsetzung teils nicht, www.heise.de 21.06.2022, Kurzlink: https://heise.de/-7146909; Janisch, Unverdächtig nach Mallorca, SZ 22.06.2022, 6).

EuGH

Kündigungsschutz für Datenschutzbeauftragte europarechtskonform

Der Europäische Gerichtshof (EuGH) bestätigte mit seinem Urteil vom 22.06.2022, dass die nationale Regelung des Bundesdatenschutzgesetzes zur Kündigung eines Mitarbeitenden mit der Funktion des Datenschutzbeauftragten mit dem europäischen Recht in Einklang steht (Az. C-534/20). Es steht demnach jedem Mitgliedstaat frei, strengere Vorschriften für die arbeitgeberseitige Kündigung eines Datenkontrolleurs vorzusehen, solange dieser seine Aufgaben im Einklang mit der DSGVO erfüllt.

Das BAG hatte dem EuGH diese Frage vorgelegt, nachdem einer „Teamleiterin Recht" bei einem Nürnberger Maschinenbauer noch in der Probezeit im Zusammenhang mit einer Umstrukturierung gekündigt und zugleich deren Benennung zur internen Datenschutzbeauftragten widerrufen wurde. Die Funktion wurde danach an eine externe Anwaltskanzlei übertragen. Das wollte die Frau nicht hinnehmen. Sie gewann beim ArbG und auch beim LAG Nürnberg. Eine ordentliche Kündigung sei nach § 38 Abs. 2 BDSG in Verbindung mit § 6 Abs. 6 Satz 2 BDSG ausgeschlossen, wenn kein wichtiger Grund vorliegt. Das BAG sah die Möglichkeit, dass das Unionsrecht abschließend sei, das in Art. 38 Abs. 3 Satz 2 DSGVO verbietet einen Datenschützer „wegen der Erfüllung seiner Aufgaben" abzuberufen oder zu benachteiligen. Überwiegend wurde schon bisher in Deutschland die Ansicht vertreten, beim deutschen Sonderkündigungsschutz handele es sich um materiell-arbeitsrechtliche Regelungen, für die keine Gesetzgebungskompetenz der Union besteht (Art. 153 AEUV). Eine Gegenansicht meinte jedoch, dass die Verknüpfung dieses Schutzes mit der Stellung des Beauftragten unionsrechtswidrig sei. Es werde ein wirtschaftlicher Druck aufgebaut, an einem einmal benannten Kontrolleur dauerhaft festzuhalten.

Gemäß dem EuGH steht Art. 38 Abs. 3 Satz 2 DSGVO nicht der Regelung entgegen, nach der einem bei einem Verantwortlichen oder einem Auftragsverarbeiter beschäftigten Datenschutzbeauftragten nur aus wichtigem Grund gekündigt werden kann, auch wenn die Kündigung nicht mit der Erfüllung seiner Aufgaben zusammenhängt. Mit der Norm solle im Wesentlichen die funktionelle Unabhängigkeit des Beauftragten gewahrt und damit die Wirksamkeit der Bestimmungen der DSGVO gewährleistet werden. Nicht bezweckt werde insgesamt das Arbeitsverhältnis zu regeln. Dieses sei allenfalls beiläufig betroffen, soweit dies für die Erreichung dieser Ziele unbedingt erforderlich sei. Es stünde jedem Mitgliedstaat frei in Ausübung seiner vorbehaltenen Zuständigkeit besondere, strengere Vorschriften für die arbeitgeberseitige Kündigung eines Datenschutzbeauftragten vorzusehen, sofern diese mit dem Unionsrecht und vor allem Art. 38 Abs. 3 Satz 2 DSGVO vereinbar sind. Ein strengerer Schutz dürfe die Verwirklichung der Ziele der DSGVO nicht beeinträchtigen. Dies wäre der Fall, wenn dieser Schutz jedwede Kündigung eines Datenschutzbeauftragten verböte, der nicht mehr die für die Erfüllung seiner Aufgaben erforderlichen beruflichen Eigenschaften besitze oder seine Aufgaben nicht im Einklang mit der DSGVO erfülle.

Der Vorsitzende des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V., Thomas Spaeing, erklärte dazu: „Wir begrüßen diese höchstrichterliche Klarstellung, die Sicherheit für die Unternehmen und ihre Mitarbeitenden gibt. Davon profitieren beide Seiten. Der benannte Datenschutzbeauftragte ist besonders wertvoll für das Unternehmen, wenn er unabhängig und zukunftsorientiert an innovativen Lösungen arbeiten kann." Die Datenschutzbeauftragten fungierten in vielen kleinen und mittelständischen Unternehmen als wesentliche Lotsen für die Digitalisierung der Prozesse und Dienstleistungen (Pressemitteilung des BvD v. 29.06.2022, Urteil des EuGH stärkt die Rolle des internen Datenschutzbeauftragten und hilft den Unternehmen; Sonderkündigungsschutz für Datenschutzbeauftragte mit Unionsrecht vereinbar, https://rsw.beck.de 23.06.2022).

EuGH-Generalanwalt

Auskunftsanspruch auch zu konkreten Datenempfängern

Betroffene, deren Daten zu Marketingzwecken weitergegeben wurden, können nach einem am 09.06.2022 vorgelegten Gutachten des zuständigen Generalanwalts am Europäischen Gerichtshof (EuGH), Giovanni Pitruzzella, Informationen über die konkreten Empfänger der Daten verlangen. Das Auskunftsrecht gemäß der Datenschutz-Grundverordnung (DSGVO) kann demgemäß nur in bestimmten Fällen auf die Kategorie von Empfängern beschränkt werden.

Ein Kläger wollte von der österreichischen Post wissen, ob und an wen das Unternehmen personenbezogene Daten

über ihn weitergegeben hat. Die Post hatte bislang nur erklärt, dass sie Daten zu Marketingzwecken an Geschäftskunden weitergegeben habe, aber keine konkreten Empfänger genannt. Der oberste Gerichtshof Österreichs setzte das Verfahren aus und bat den EuGH um eine Auslegung der DSGVO. Laut den Schlussanträgen von Pitruzzella müssen Betroffene grundsätzlich das Recht haben Informationen über die konkreten Empfänger zu bekommen, da nur so mögliche weitere Rechte wie die Löschung oder Berichtigung von Daten geltend machen können. Eine Ausnahme sei nur möglich, wenn die Anträge auf Auskunft nachweisbar unbegründet oder exzessiv seien oder wenn es unmöglich sei die konkreten Empfänger herauszufinden. Dann könne sich das Auskunftsrecht auf die Empfängerkategorie beschränken.

Die Richter am EuGH sind an das Gutachten des Generalanwalts nicht gebunden, orientieren sich aber in der Regel daran. Ein Termin für die Urteilsverkündung wurde noch nicht veröffentlicht (EuGH: Auskunftsrecht bei Datenweitergabe umfasst konkrete Empfänger, Digitalisierung & KI, Tagesspiegel Digitalpolitik 10.06.2022).

BVerfG

Vorläufiger Rechtsschutz wegen BSI-Warnung vor Kaspersky abgelehnt

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) darf vorerst gemäß einem Beschluss des Bundesverfassungsgerichts (BVerfG) vom 02.06.2022 weiter vor der Virenschutzsoftware des russischen Anbieters Kaspersky warnen (Az. 1 BvR 1071/22). Das Gericht nahm eine Klage der deutschen Tochtergesellschaft nicht zur Entscheidung an. Damit hat sich der mit der Verfassungsbeschwerde verbundene Eilantrag erledigt. Es sei „nicht unzumutbar eine Entscheidung in der Hauptsache vor den Verwaltungsgerichten abzuwarten".

Das BSI hatte am 15.03.2022 vor dem Hintergrund des russischen Angriffskriegs gegen die Ukraine empfohlen Virenschutzsoftware von Kaspersky durch alternative Produkte zu ersetzen. Es bestehe ein erhebliches Risiko „eines erfolgreichen IT-Angriffs", an dem ein russischer Hersteller gegen seinen Willen als Werkzeug oder aktiv beteiligt sein könnte. Kaspersky hatte von einer Entscheidung aus politischen Gründen gesprochen und dagegen geklagt. Das Kölner Verwaltungsgericht lehnte einen Eilantrag Anfang April ab (Az. 1 L 466/22), eine Beschwerde zum nordrhein-westfälischen Oberverwaltungsgericht blieb erfolglos (Az. 4 B 473/22).

Die Kammer des BVerfGs meinte, Kaspersky habe „nicht ausgeführt, dass die Verwaltungsgerichte gerade durch die Art und Weise der Bearbeitung des Antrags auf Erlass einer einstweiligen Anordnung Grundrechte verletzt haben". Erst die eingehende Prüfung der Sach- und Rechtslage versetze das Bundesverfassungsgericht in die Lage die grundrechtsrelevanten Fragen entscheiden zu können. Die tatsächlichen Umstände der Sicherheit der Software müssten zunächst von den zuständigen Fachgerichten aufgeklärt werden (Klage abgelehnt: BSI darf vorerst weiter vor Kaspersky-Virenschutz warnen, www.heise.de 10.06.2022, Kurzlink: https://heise.de/-7136938).

BVerfG

Keine Datenhehlerei bei journalistischer Recherche

Das Bundesverfassungsgericht (BVerfG) hat in einem Beschluss klargestellt, dass sich Journalistinnen und Journalisten nicht strafbar machen, wenn sie „geleakte" Daten entgegennehmen. Das Gericht nahm formal die von der Gesellschaft für Freiheitsrechte (GFF) koordinierte Verfassungsbeschwerde gegen den Straftatbestand der Datenhehlerei in § 202d Strafgesetzbuch (StGB) nicht zur Entscheidung an. In der Begründung legt es die Ausnahme von der Strafbarkeit für Journalistinnen und Journalisten weit aus und stärkt damit die Pressefreiheit.

Die GFF hatte die Klage 2017 im Namen von netzpolitik.org, Reporter ohne Grenzen sowie sieben Journalisten und Bloggern erhoben, die selbst regelmäßig investigativ und mithilfe geleakter Daten recherchieren. Dazu gehören unter anderem Markus Beckedahl, Andre Meister (netzpolitik.org), Peter Hornung (NDR, Panama Papers) und Hajo Seppelt (ARD, Olympia-Doping). Auch Redakteure von c't und heise online wirkten mit.

David Werdermann, Rechtsanwalt und Projektkoordinator der GFF, erläuterte: „Das Bundesverfassungsgericht hat mit seiner Entscheidung klargestellt, dass sich Journalist*innen nicht strafbar machen, wenn sie Daten von Whistleblowerinnen und Whistleblowern entgegennehmen. Unsere Verfassungsbeschwerde hat damit ihr Hauptziel erreicht, auch wenn sie formal nicht zur Entscheidung angenommen wurde: Die Gefahr der Strafverfolgung journalistischer Kerntätigkeiten und der Durchsuchung von Redaktionsräumen ist entschärft."

Der 2015 eingeführte Datenhehlerei-Paragraf (§ 202d StGB) stellt den Umgang mit Daten unter Strafe, die zuvor jemand rechtswidrig erlangt hat. Die Norm sollte nach Absicht des Gesetzgebers vorrangig den Handel mit gestohlenen Kreditkarten- oder Nutzerdaten bekämpfen. Aufgrund der ungenauen Formulierung des Gesetzes erfasst sie darüber hinaus aber auch das Sich-Verschaffen, die Überlassung und Verbreitung elektronisch gespeicherter Daten, die von Whistleblowerinnen und Whistleblowern weitergegeben wurden. Auch aufgrund massiver Kritik von Presse-Verbänden beschloss der Bundestag eine Ausnahme für Journalistinnen und Journalisten: Er beschränkte diese jedoch auf berufliche Handlungen, mit denen Daten entgegengenommen, ausgewertet oder veröffentlicht werden. Gemäß BVerfG drängt sich damit aber auf, „dass ein umfassender Ausschluss journalistischer Tätigkeiten bezweckt wird". Der Tatbestandsausschluss ziele darauf ab, dass eine journalistische Tätigkeit auch dann nicht unter Strafe gestellt wird, wenn Recherchen gegebenenfalls unergiebig sind und es im Ergebnis nicht zu einer Veröffentlichung kommt.

Die Verfassungsbeschwerden dreier weiterer Beschwerdeführer wurden vom Verfahren abgetrennt und sind noch beim Zweiten Senat des Bundesverfassungsgerichts anhängig. Dazu gehören der GFF-Vorsitzende Dr. Ulf Buermeyer

sowie ein Anwalt und ein IT-Experte, die jeweils regelmäßig investigativ arbeitende Medien beraten. Von der ausstehenden Entscheidung erhofft sich die GFF eine Klarstellung, dass auch journalistischen Hilfspersonen keine Strafverfolgung droht (Knaack, Pressefreiheit: Bundesverfassungsgericht entschärft Datenhehlerei-Paragraf, www.heise.de 16.06.2022, Kurzlink: https://heise.de/-7142362; Erfolg für die Pressefreiheit: Bundesverfassungsgericht entschärft Datenhehlerei-Paragraf, freiheitsrechte.org 16.06.2022).

BGH

Keine E-Mail-Inbox-Werbung ohne wirksame Einwilligung

Gemäß einem Urteil des Bundesgerichtshofs (BGH) vom 13.01.2022 dürfen webbasierte E-Mail-Dienste wie T-Online, GMX, web.de oder Gmail Nutzern kostenloser Basisvarianten nicht einfach Werbenachrichten direkt in der Inbox anzeigen (Az. I ZR 25/19). Diese umstrittene Praxis erfordert eine explizite, informierte Einwilligung im Sinne der Datenschutz-Grundverordnung (DSGVO). In dem rechtskräftig entschiedenen Fall beanstandeten die Städtischen Werke Lauf a.d. Pegnitz (StWL) vor deutschen Gerichten eine einschlägige Werbemaßnahme des konkurrierenden Stromlieferanten Eprimo aus der Eon-Gruppe. Dieser hatte eine Werbeagentur beauftragt, mit dem Hinweis „Anzeige" versehene Werbeeinblendungen in E-Mail-Postfächern von Nutzern des kostenlosen E-Mail-Dienstes T-Online zu schalten. Vergleichbare Inbox-Werbung ist bei vielen Anbietern üblich.

Nach Ansicht der Stadtwerke verstößt diese Maßnahme gegen das Gesetz gegen den unlauteren Wettbewerb (UWG). Die beanstandete Werbetechnik unterscheidet sich zwar vom technischen Modell der E-Mail, ist aber aus dem Horizont des Empfängers der unerwünschten E-Mail (Spam) zum Verwechseln ähnlich. Die StWL nahmen Eprimo daher vor dem Landgericht Nürnberg-Fürth auf Unterlassung in Anspruch. Dieses gab der Klage statt und verurteilte Eprimo eine solche Werbung zu unterlassen, da diese eine unzumutbare Belästigung darstelle und irreführend sei.

Im Berufungsverfahren hatte das Oberlandesgericht Nürnberg der Beklagten Recht gegeben. Der BGH, bei dem der Streit in der Revision landete, legte dem Europäischen Gerichtshof (EuGH) daraufhin Fragen zur Interpretation des EU-Rechts vor. Dieser entschied im November 2021, dass die E-Privacy-Richtlinie darauf abzielt Teilnehmer gegen die Verletzung ihrer Privatsphäre durch unerbetene Nachrichten für Zwecke der Direktwerbung zu schützen. Ein ohne Zwang erfolgendes Opt-in sei daher nötig. Inbox-Werbung behindere den Zugang zu den eigentlichen E-Mails, ähnlich wie Spam.

Der BGH wies die Berufung von Eprimo gegen das Urteil des Landgerichts daraufhin zurück. Er legte die Kosten der Rechtsmittel der Beklagten auf. Diese muss zudem die Abmahnkosten in Höhe von 1.531,90 Euro nebst Zinsen zahlen. Eine erneute Verhandlung des Streits vor dem Oberlandesgericht hielten die Karlsruher Richter nicht für nötig.

Eine wirksame Einwilligung in eine Inbox-Werbung liegt laut dem BGH-Urteil nicht vor, wenn der Nutzer eines kostenlosen E-Mail-Dienstes „sich allgemein damit einverstanden erklärt Werbeeinblendungen zu erhalten", um kein Entgelt zahlen zu müssen. Erforderlich sei vielmehr, dass der Betroffene vor einer Zustimmung „klar und präzise über die genauen Modalitäten der Verbreitung einer solchen Werbung und insbesondere darüber informiert wird, dass Werbenachrichten in der Liste der empfangenen privaten E-Mails angezeigt werden".

Der von den Stadtwerken geltend gemachte Unterlassungsanspruch könne gemäß § 7 UWG, der eine einschlägige Klausel der E-Privacy-Richtlinie umsetzt, nicht verneint werden. Die allgemeinen Voraussetzungen dafür lägen unter dem Gesichtspunkt der unzumutbaren Belästigung vor. Es handle sich um eine unzulässige geschäftliche Handlung.

Im vorliegenden Fall wurde die Werbenachricht den Karlsruher Richtern zufolge aus der Sicht des Adressaten in der Inbox des E-Mail-Systems – also in einem normalerweise privaten Nachrichten vorbehaltenen Bereich – angezeigt. Der Nutzer konnte diesen Sektor erst nach Überprüfung des Inhalts der Reklame und nur durch aktives Löschen derselben freimachen, um einen Überblick über seine ausschließlich privaten E-Mails zu erhalten. Die Einblendung habe so den Zugang zur eigentlichen E-Post in ähnlicher Weise behindert wie bei unerbetenen E-Mails (Spam). Dies sei nur mit dem vorherigen ausdrücklichen Plazet der Teilnehmer gestattet.

Laut der relevanten DSGVO bezeichne der Ausdruck „Einwilligung" jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung. Der Nutzer müsse sein Opt-in „für den konkreten Fall und in voller Kenntnis der Sachlage bekundet" haben. Einschlägige E-Mail-Anbieter wie GMX und web.de passten ihre Einwilligungserklärungen unmittelbar nach der Veröffentlichung des Urteils an. So findet sich darin nun auch eine Klausel für Inbox-Werbung. Alternativ besteht die Möglichkeit die Gratisvarianten der Dienste mit personalisierten klassischen Banneranzeigen weiter zu verwenden (Bundesgerichtshof: Unerwünschte Inbox-Werbung ist genauso rechtswidrig wie Spam, www.heise.de 04.06.2022, Kurzlink: https://heise.de/-7132364).

OVG Münster

Postanschrift für IFG-Antrag nicht immer erforderlich

Das Bundesministerium des Innern und für Heimat (BMI) darf gemäß einem Urteil des Oberverwaltungsgerichts (OVG) NRW vom 15.06.2022 nicht standardmäßig die Angabe der Postanschrift des Antragstellers verlangen, der über die Internetplattform fragdenstaat.de einen Antrag auf Informationszugang nach dem Informationsfreiheitsgesetz (IFG) stellt (16 A 857/21). Das OVG änderte damit eine vorangegangene Entscheidung des Verwaltungsgerichts (VG) Köln ab (13 K 1190/20).

Ein Bürger hatte mittels einer von der Internetplattform fragdenstaat.de generierten, nicht personalisierten

E-Mail-Adresse beim BMI einen Auskunftsantrag nach dem IFG gestellt. Das Ministerium forderte ihn dazu auf seine Postanschrift mitzuteilen, da andernfalls der verfahrensbeendende Verwaltungsakt nicht bekanntgegeben und das Verfahren nicht ordnungsgemäß durchgeführt werden könne. Aufgrund dessen sprach der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) eine datenschutzrechtliche Verwarnung gegenüber dem BMI aus. Das Verwaltungsgericht Köln gab der dagegen gerichteten Klage des BMI statt und hob die Verwarnung auf. Die Berufung des BfDI hatte Erfolg.

Das OVG begründete seine Entscheidung damit, dass die Erhebung der Postanschrift im Zeitpunkt der Datenverarbeitung für die vom BMI verfolgten Zwecke nicht erforderlich war. Weder aus den maßgeblichen Vorschriften des IFG noch aus den Grundsätzen des Allgemeinen Verwaltungsrechts geht hervor, dass ein Antrag nach dem IFG stets die Angabe einer Postanschrift erfordert. Anhaltspunkte dafür, dass eine Datenerhebung im vorliegenden Einzelfall erforderlich war, liegen ebenfalls nicht vor. Wegen der grundsätzlichen Bedeutung wurde die Revision zum Bundesverwaltungsgericht zugelassen.

In einem weiteren, auf einem vergleichbaren Sachverhalt beruhenden Verfahren hatten der BfDI und die beigeladene Open Knowledge Foundation, die die Internetplattform fragdenstaat.de betreibt, mit ihren Berufungen hingegen keinen Erfolg. Der BfDI hatte dem BMI die datenschutzrechtliche Anweisung erteilt in Verfahren nach dem IFG über die vom Antragsteller übermittelten Kontaktdaten hinaus nur noch dann zusätzliche personenbezogene Daten zu verarbeiten, wenn ein Antrag ganz oder teilweise abzulehnen sein wird oder wenn Gebühren zu erheben sind. Wie schon das VG Köln (13 K 1189/20) hielt auch das OVG in seinem Urteil diese Anweisung für rechtswidrig, da der streitgegenständliche Bescheid jedenfalls einen zu weitreichenden Regelungsgehalt habe. Dieser verbietet eine Datenverarbeitung auch für die Fälle, in denen sie ausnahmsweise gerechtfertigt sein könnte. In diesem Verfahren hat das OVG die Revision nicht zugelassen (Standardmäßige Erhebung der Postanschrift des Antragstellers bei IFG-Antrag über fragdenstaat.de unzulässig, www.ovg.nrw.de 15.06.2022).

LAG Baden-Württemberg

Korrekte BEM-Information Voraussetzung für krankheitsbedingte Kündigung

(tw) Das Landesarbeitsgericht Baden-Württemberg (LAG) hat mit rechtskräftigem Urteil vom 20.10.2021 eine krankheitsbegründete Kündigung aufgehoben, weil die eingeforderte Einwilligungserklärung zur Verarbeitung von Gesundheitsdaten im sog. BEM-Verfahren nicht datenschutzkonform war (Az. 4 Sa 70/20). Das Gericht bestätigte und präzisierte damit ein Urteil vom 28.07.2021 (Az. 4 Sa 68/20).

Der Arbeitgeber hatte einem Beschäftigten krankheitsbedingt im Juni 2020 gekündigt, nachdem dieser in den Jahren 2016 bis 2019 jeweils mehr als 30 Arbeitstage (6 Wochen) arbeitsunfähig geschrieben war, sich auch im Januar 2020 krankgemeldet hatte und der Arbeitgeber hierfür jeweils Entgeltfortzahlung leisten musste. Zuvor hatte der Arbeitgeber den Beschäftigten erneut zum betrieblichen Eingliederungsmanagement (BEM) eingeladen und von diesem keine Rückmeldung erhalten. In dieser Einladung war darauf hingewiesen worden, dass der Beschäftigte der Verarbeitung seiner Gesundheitsdaten durch den Vorgesetzten sowie durch ein Integrationsteam, dem der Leiter des örtlichen Standortes angehöre, im Rahmen des BEM-Verfahrens zustimmen müsse. Das Arbeitsgericht Reutlingen hatte den Arbeitgeber zur Weiterbeschäftigung verurteilt, weil die berücksichtigungsfähige Überschreitung des Sechswochenzeitraums der Arbeitsunfähigkeit pro Kalenderjahr nicht so gravierend sei, dass die weitere Beschäftigung unzumutbar ist. Das Landesarbeitsgericht (LAG) bestätigte die Rechtswidrigkeit der Kündigung, allerdings mit einer völlig anderen Begründung:

Eine mit Krankheitsausfall begründete ordentliche Kündigung setzt eine negative Gesundheitsprognose voraus, also objektive Tatsachen, die – auch bei Kurzerkrankungen – eine weitere negative Entwicklung erwarten lassen. Die prognostizierten Fehlzeiten müssen zu einer Beeinträchtigung betrieblicher Interessen führen, was mit der Entgeltfortzahlung begründet werden kann. Gemäß dem LAG muss im Rahmen einer Interessenabwägung diese Beeinträchtigung für den Arbeitgeber so schwer sein, dass sie nicht hinnehmbar ist. Zwar waren im konkreten Fall frühere Fehlzeiten auf zwei Krankheiten zurückzuführen, die letztlich vollständig ausgeheilt waren. Diese durften nicht mehr mitgerechnet werden. Doch auch unter Abzug dieser Fehlzeiten lagen die Fehlzeiten in den letzten 4 Jahren jeweils noch über 30 Tagen, ohne abnehmende Tendenz. Dies sei für den Arbeitgeber nicht weiter zumutbar.

Obwohl damit die Voraussetzungen für eine krankheitsbedingte Kündigung im Prinzip vorlagen, erklärte das LAG die Kündigung für nicht sozial gerechtfertigt, weil das BEM-Verfahren nicht ordnungsgemäß eingeleitet worden war. Die Durchführung des BEM-Verfahrens ist keine formelle Wirksamkeitsvoraussetzung für eine Kündigung. Es ist aber bei der Verhältnismäßigkeitsprüfung relevant. Mit Hilfe des BEM können mildere Mittel als eine Kündigung gefunden werden. Kann der Arbeitgeber nachweisen, dass das BEM z.B. durch eine leidensgerechte Anpassung des Arbeitsplatzes oder eine geänderte Tätigkeit an den Fehlzeiten nichts Wesentliches ändern würde, dann kann das Unterbleiben des BEM für ihn nicht zum Nachteil gewertet werden. Ist aber nicht auszuschließen, dass nach Durchführung des BEM eine Weiterbeschäftigung möglich wäre, dann muss dem Beschäftigten ein ordnungsgemäßes BEM angeboten werden, da das Ziel des BEM ist festzustellen, aufgrund welcher gesundheitlicher Einschränkungen die bisherigen Ausfallzeiten entstanden sind und mit welchen Veränderungen die krankheitsbedingten Fehlzeiten für den Arbeitgeber hinnehmbar reduziert werden können.

Zentrale Voraussetzung eines ordnungsgemäßen BEM ist, dass angesichts der zu erhebenden sensitiven Daten der Betroffene über diese Daten sowie über deren erforderliche Kenntnisnahme und weitere Verarbeitung durch die eingebundenen Stellen und Personen korrekt hingewiesen wird. Nur so kann er infor-

miert in diese Verarbeitung einwilligen. Diese Einwilligung ist Voraussetzung für die zulässige BEM-Datenverarbeitung. Dem Arbeitnehmer muss also mitgeteilt werden, welche Krankheitsdaten erhoben und gespeichert und inwieweit und für welche Zwecke sie dem Arbeitgeber zugänglich gemacht werden.

Im konkreten Verfahren konnte nicht festgestellt werden, ob das Einladungsschreiben dem Beschäftigten zugestellt worden war. Darauf kam es dem LAG aber gar nicht an, da selbst bei korrekter Zustellung keine ordnungsgemäße Unterrichtung stattgefunden hätte: In der Unterrichtung war aufgeführt, dass die sensitiven Daten auch gegenüber dem „Vorgesetzten" und der „Standortleitung" bekannt gemacht würden. Zumindest der Standortleitung hätten aber die Daten, z.B. die Diagnosen, in keinem Fall mitgeteilt werden müssen und dürfen. Durch die Einbeziehung der Standortleitung in den potenziellen Empfängerkreis der Daten hätte der Betroffene berechtigterweise seine Zustimmung zum BEM verweigern können, da diese nicht erforderlich war.

Obwohl der gekündigte Beschäftigte die Fehlerhaftigkeit der BEM-Einladung im Verfahren nicht gerügt hatte, begründete das LAG damit die Unzulässigkeit der Kündigung: „Es kann vorliegend nicht ausgeschlossen werden, dass bei einer ordnungsgemäßen Unterrichtung über das BEM der Kläger an einem solchen teilgenommen hätte und im Rahmen des Verfahrens Möglichkeiten gefunden worden wären die Fehlzeiten des Klägers zu reduzieren".

Durch eine Betriebsvereinbarung können die Rahmenbedingungen des BEM präziser als im Gesetz festgelegt werden. Dadurch wird für den Arbeitgeber wie für den Beschäftigten mehr Rechtssicherheit geschaffen. Das Verfahren muss so gestaltet sein, dass nur Daten erhoben, verarbeitet und an Dritte weitergeleitet werden, die für das Gelingen des BEM erforderlich sind. Davon kann man bei Vorgesetzten grundsätzlich nicht ausgehen. Der Betroffene muss der gesamten Durchführung des BEM zustimmen und damit auch seine Einwilligung in die sensitive Datenverarbeitung geben. Diese Einwilligung ist nur begrenzt freiwillig; Eine Verweigerung der Einwilligung in eine erforderliche Datennutzung kann zum Scheitern des BEM führen, was evtl. letztlich bei einer Kündigung gegen den Betroffenen verwendet wird.

VG Ansbach

Keine pauschale Videoüberwachung im Fitnessstudio

Das Verwaltungsgericht (VG) Ansbach hat mit Urteil vom 23.02.2022 entschieden, dass eine Videoüberwachung in Fitnessstudios nur unter ganz bestimmten Umständen und Voraussetzungen zulässig ist (Az. AN 14 K 20.00083). Die Betreiberin eines Fitnessstudios hatte sechs Videokameras ohne Tonaufzeichnung installiert, um verschiedene Bereiche des Studios abzudecken. Das zuständige Bayerische Landesamt für Datenschutzaufsicht (BayLDA) betrachtete dies als unzulässig und forderte sie auf die Videoüberwachung einzustellen.

Das VG sah in diesem Fall keine datenschutzrechtlich konforme Einwilligung. Die Tatsache, dass an gewissen Stellen auf die Videoüberwachung hingewiesen würde, begründe keine konkludente Einwilligung der Trainierenden. Dafür fehle es an einer eindeutigen Handlung seitens der Betroffenen. Gerade Stillschweigen und Untätigkeit könnten keine Einwilligung darstellen.

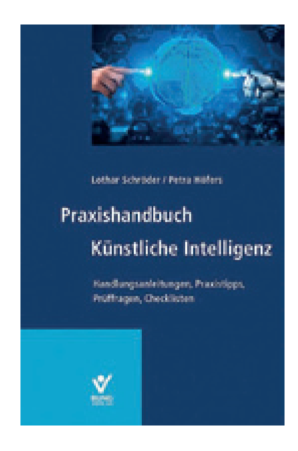
Auch eine vertragliche Legitimation akzeptierte das VG nicht (Art. 6 Abs. 1 lit. b DSGVO). Als Fitnessstudiobetreiber habe man durchaus dafür Sorge zu tragen, dass die Kundschaft in gewissem Umfang vor Diebstählen und Übergriffen geschützt ist. Dies begründe eine sogenannte vertragliche Nebenpflicht (Rücksichtnahme- und Schutzpflichten) aus dem Fitnessstudiovertrag. Eine umfassende und weitgehende Videoüberwachung sei damit jedoch nicht zu begründen. Der Studiobetreiber sei grundsätzlich nur dazu verpflichtet für ein Schutzniveau zu sorgen, mit welchem der durchschnittliche Besucher rechnen könne, also z.B. dem Aufstellen von absperrbaren Spinden. Mit einer lückenlosen Videoüberwachung könne ein Trainierender jedoch keineswegs rechnen.

Die Besitzerin des Fitnessstudios versucht die Erfassung gemäß Art. 6 Abs. 1 lit. f DSGVO damit zu rechtfertigen, dass dies der Prävention und Aufklärung von Diebstählen und Sachbeschädigungen diene, welche es zuvor vermehrt gegeben hätte. Außerdem hätten mildere Mittel wie Warnschilder keinen Erfolg gehabt. Darüber hinaus könne man dadurch weibliche Trainierende vor sexuellen Übergriffen schützen, denn es könne nicht zu jeder Zeit in jedem Teil des Studios Personal sein. Angesichts des tiefen Eingriffs in Rechte der Betroffenen verlangt das VG für die Wahrnehmung eines berechtigen Interesses eine Verhältnismäßigkeit der Maßnahme. Diese muss einen legitimen Zweck verfolgen und überdies geeignet, erforderlich und angemessen sein. Ansonsten ist diese datenschutzwidrig. Eine umfassende lückenlose Videoüberwachung sei in der Regel unzulässig; die Überwachung sei auf die besonders gefährdeten Bereiche zu begrenzen (Wehowsky, VG Ansbach: Keine pauschale Videoüberwachung in Fitnessstudios, www.iitr.de 30.06.2022).



Bild: iStock.com/ golubovy

Buchbesprechungen



Schröder, Lothar/Höfers, Petra
Praxishandbuch Künstliche Intelligenz
Handlungsanleitungen, Praxistipps, Prüffragen, Checklisten
Bund-Verlag, 2022,
ISBN 978-3-7663-7264-2
452 S., 48 €

(tw) Mit dem Betriebsrätemodernisierungsgesetz fand der Begriff „Künstliche Intelligenz“, abgekürzt „KI“, 2021 Eingang ins Betriebsverfassungsgesetz: Beim Einsatz von KI hat der Betriebsrat Anspruch auf Hinzuziehung von Sachverstand. Wird KI in Bewerbungsverfahren verwendet, dann besteht eine Mitbestimmungspflicht. Schon erheblich früher hat das, was landläufig unter KI verstanden wird, in vielen Betrieben Einzug gehalten. Sie beeinflusst den betrieblichen Alltag massiv – im positiven wie im negativen Sinne. Dabei geht es um erhöhte Produktivität, um die Entlastung von Mitarbeitern und die Qualifizierung von Jobs. Und es geht um Gefahren für den Datenschutz, die Verhinderung von maschinellen Verhaltens- und Leistungskontrollen, aber auch um die Vermeidung von Diskriminierung, um Arbeitsbedingungen und Arbeitsschutz.

Insofern ist das Buch von Schröder/Höfers überfällig. Aber es kommt nicht zu spät, ja vielleicht gerade zum richtigen Zeitpunkt, wo die KI eben ins BetrVG Eingang gefunden hat und von der EU-Kommission der Entwurf für eine KI-Verordnung vorgelegt wurde. Beides ist hier umfassend berücksichtigt. Es bestehen erste anwendbare rechtliche Grundlagen; es gibt eine umfassende Diskussion über KI im Beschäftigungsverhältnis und es gibt Konzepte im Umgang hiermit. All das ist von großer Relevanz für Betriebs- und Personalräte.

Und all das finden wir in dem Werk von Schröder und Höfers, das durch Gastbeiträge von Cristian Benner, Karl-Heinz Brandl, Frank Bsirske, Reiner Hoffmann, Markus Hoppe und Christoph Schmitz bereichert wird. Es nennt sich tiefstapelnd „Praxishandbuch“ und ist doch erheblich mehr. Natürlich adressiert es vorrangig Betriebs- und Personalräte – und dies in einer leicht verständlichen und lebendigen Sprache, zugleich mit viel Detailwissen. Es adressiert aber auch Personalleiter, Unternehmensleiter, IT-Spezialisten, Juristen und ist selbst für die wissenschaftliche Arbeit zum Thema eine hervorragende Grundlage. Dies liegt daran, dass das Thema generell umfassend behandelt wird, um sich dann auf den betrieblichen Einsatz zu fokussieren. Dies liegt auch daran, dass wissenschaftliche, politische und juristische Quellen umfassend ausgewertet und dokumentiert werden.

Dabei bleibt aber immer der praktische Ansatz im Blick. Dies beginnt mit der Dokumentation der einschlägigen Rechtsquellen und Dokumente, setzt sich fort in vielen Checklisten und Ratschlägen und gibt den Beschäftigtenvertretungen ausführliche Fragenkataloge an die Hand, mit denen sie KI hinterfragen und bewerten können. Das Buch vermittelt Qualitätsfaktoren und Gestaltungsbeispiele und beschreibt dabei die technischen, ethischen und sozialen Zusammenhänge. Ein KI-Lagom-Ansatz zur Qualitätsprüfung von KI wird vorgestellt ebenso wie ein Beschäftigtendatenschutz-Index (BeDaX), mit dem eine datenschutzrechtliche Bewertung im Arbeitsverhältnis mit Hilfe von detaillierten Indikatoren angestrebt wird. Dabei wird aber nie eine verengte Sichtweise präsentiert, sondern immer eine umfassende Darstellung, die von den Grundrechten und ethischen Anforderungen bis hin zu konkreten Ausgestaltungen von Software und Verfahren führt. Kurzum: Das Buch ist ein absolutes Muss für Menschen, die sich professionell mit KI im Betrieb befassen, und allen dringend zu empfehlen, die damit in Berührung kommen. Ein detailliertes Inhaltsverzeichnis erschließt die Inhalte bei spontanen Fragestellungen; ein aktuelles Literaturverzeichnis gibt Hinweise für weitere Recherchen.



Wolff, Heinrich Amadeus/
Brink, Stefan (Hrsg.)
Datenschutzrecht
DS-GVO, BDSG, Grundlagen, Bereichsspezifischer Datenschutz, Kommentar
2. Aufl. 2022, C.H.Beck München
ISBN 978 3 406 78990 8, 1763 S.,
169,00 €

(tw) Der Beck-Verlag ist in Sachen Literatur zum Datenschutz Marktführer. U.a. mit Paal/Pauly, Gola, Ehmann/Selmayr und Kühling/Buchner liefert er für jeden Geschmack und in jedem Umfang etwas zu DSGVO & Co. Nun bringt er mit dem Wolff/Brink ein weiteres gedrucktes Werk auf den Markt. Die erste Auflage hatte noch den Titel „Datenschutzrecht in Bund und Ländern“ und war schon 2013 voluminös. Jetzt steht die DSGVO im Vordergrund, das Landesdatenschutzrecht spielt praktisch keine Rolle mehr. Der Umstand, dass der „Wolff/Brink“ erst nach 9 Jahren eine gedruckte Neuauflage findet, hat

den einfachen Hintergrund: Das Werk war über die ganzen Jahre als Online-Kommentar im Internet abrufbar. Der Verlag will nun auch die weniger digital arbeitenden Datenschutzjuristen bedienen, von denen es offenbar immer noch genug gibt.

Das Konzept ist geblieben. Gestartet wird mit ca. 230 Seiten „Grundlagen und bereichsspezifischer Datenschutz“; es folgen 880 Seiten DSGVO; dem BDSG werden ca. 610 Seiten gewidmet. Die Beiträge sind weitestgehend auf dem aktuellen Stand in Bezug auf Gesetzgebung, Rechtsprechung und Spruchpraxis der Aufsichtsbehörden. Das neue TTDSG ist zwar berücksichtigt, aber nicht kommentiert. Einige bereichsspezifische Darstellungen, die noch 2013 abgedeckt waren, bleiben „unbesetzt“: Geliefert werden Prinzipien, Völkerrecht und supranationale Grundlagen, Justiz, freie Berufe, Medien und Telekommunikation, Finanzwesen und Sicherheitsbehörden. Unbesetzt bleiben u.a. das Landesrecht, die Werbung, Versicherungen und der Sozialdatenschutz. Datenschutz ist offenbar zu komplex und zu umfangreich, um insgesamt zwischen zwei Buchdeckel zu passen.

Bei der Rezension eines derart dicken Werks ist ein Eingehen auf spezifische Inhalte kaum möglich. Wohl kann aber gesagt werden, dass alle behandelten Themen nicht nur aktuell, sondern auch hochkompetent und hinsichtlich der Quellen sehr vollständig behandelt werden. Das hat seinen Grund auch darin, dass sich die Autorenliste wie das „who is who“ des rechtlichen Datenschutzes liest. Dabei fällt auf, dass Autoren, ja selbst Herausgeber von anderen Datenschutz-Kommentaren und -Handbüchern auch hier zu Wort kommen: Anwälte, Aufsichtsbehörden-Beschäftigte, Professoren, Unternehmensjuristen, wissenschaftliche Assistenten, Richter. D.h. nicht nur die Blickrichtung, auch die Positionen zum Datenschutz sind stark davon abhängig, wer das Thema bearbeitet. Wolff war bisher Rechtsprofessor und wurde eben Richter am Bundesverfassungsgericht. Brink hat sich als Datenschutzbeauftragter von Baden-Württemberg profiliert, will aber in Kürze wechseln (s.o. S. 184).

Das Werk verfolgt das Ziel auf praktische Rechtsfragen Antworten zu geben. Meinungsverschiedenheiten werden angesprochen. Durch die umfassende Rezeption von Literatur ist das Werk auch wissenschaftlich nutzbar, wenn auch die Tiefe des Simitis/Hornung/Spiecker (DANA 1/2019, 54) zumeist nicht erreicht wird. Das Datenschutzrecht ist eine äußerst lebendige Rechtsmaterie; hier wird einem ein aktueller Diskussionsstand geboten. Keine Gewähr besteht, dass dabei dann immer eine bürgerrechtsorientierte Sicht präsentiert wird. So bietet das Werk einen guten Überblick über die üppige und stark redundante Datenschutzliteratur.



Kerth, Cornelia/Kutscha, Martin (Hrsg.)
Was heißt hier eigentlich Verfassungsschutz?
Ein Geheimdienst und seine Praxis
PapyRossa Verlag Köln, 2020
ISBN 978-3-89438-729-7,
148 S., 12,90 €

(tw) Das Bundesamt für Verfassungsschutz – das BfV, der innerdeutsche nationale Geheimdienst – ist in vieler Hinsicht schon lange nicht mehr geheim, aber er agiert weiterhin im Geheimen. Daher ist es dringend nötig sich immer wieder mit diesem Dienst in unserer demokratischen und freiheitlichen Gesellschaft auseinanderzusetzen. Das tut der kleine, leicht zu lesende und hoch informative Sammelband, in dem teils prominente Kritiker des institutionalisierten bzw. so genannten Verfassungsschutzes zu Wort kommen: Neben den beiden Herausgebern, die für die Vereinigung der Verfolgten des Naziregimes – Bund der Antifaschisten (VVN-BdA) und die Humanistische Union (HU) sprechen, Rolf Gössner, Antonia von der Behrens, Luca Heyer, Klaus Stein, Niklas Schrader, Till Müller-Heidelberg, Udo Kauß und Martina Renner. Einige der Autoren sind selbst Ausgespähte der Dienste.

In den Einzelbeiträgen wird dargelegt, was der Begriff „Verfassungsschutz“ verschleiert und beschönigt, wie er gegen Extremisten vorgeht und dabei auf dem rechten Auge eher blind und auf dem linken Auge dafür hoch aktiv – und damit antidemokratisch – vorgeht, wie dort V-Leute geführt werden und welche Rolle die Ämter in der Berufsverbotepraxis hatten. Die verschleiernde Tätigkeit in Schulen wird beschrieben sowie die unsägliche Praxis Organisationen aus der Gemeinnützigkeit zu kegeln. Schließlich wird dargelegt, vor welche Probleme und Unmöglichkeiten die gerichtliche und die parlamentarische Kontrolle gestellt ist.

Das Taschenbuch ist parteiisch. Das will es auch sein. Daher geht es ihm auch nicht darum eine umfassende Darstellung des BfV und seiner kleinen Geschwister – Länderämter und Militärischer Abschirmdienste – vorzunehmen. Es plädiert – teils explizit, teils implizit – für die Abschaffung dieser Dienste und suggeriert, dass sie nicht reformierbar seien. Es gibt Gründe das anders zu sehen, so etwa die jüngste Rechtsprechung des Bundesverfassungsgerichts (DANA 2/2022, 127 f.), versuchte neue Ansätze, etwa beim Landesamt in Bremen oder in Thüringen, oder eine verstärkte Beobachtung von Rechtsradikalen. Thomas Haldenwang ist nicht Hans-Georg Maaßen. Was in dem Büchlein auch nicht thematisiert wird, ist die Frage, ob „der Verfassungsschutz“ in bestimmten Bereich jetzt schon oder künftig eine wichtige Funktion erfüllen kann, etwa bei der Bekämpfung des Islamismus oder des Terrorismus.

Der rot-grün-gelbe Koalitionsvertrag weist nicht darauf hin, dass absehbar eine Abschaffung der Verfassungsschutzämter ansteht (DANA 1/2022, 23). Insofern sind aber Reformen umso dringlicher, mit denen die Befugnisse eingehegt, die Kontrolle verbessert und die demokratische Transparenz erhöht werden. Und hierfür ist die vorliegende faktenreiche Sammlung eine wichtige Erinnerung und zugleich Bestandsaufnahme – um keinen Illusionen aufzusitzen und um Defizite zu erkennen und anzugehen.



Hamacher, Andreas/Krings, Günter/
Otto, Sven-Joachim
Glücksspielrecht – Handkommentar
Nomos Verlagsgesellschaft Baden-Baden, 2022,
716 S., 138,00 €, ISBN 978-3-8487-7934-5

(tw) Es mag überraschen in einer Datenschutzzeitschrift eine Buchbesprechung zum Glücksspielrecht zu finden. Dass beides etwas miteinander zu tun hat, erschließt sich nicht auf den ersten Blick. Datenschutz ist oft ein Glücksspiel… Aber darum geht es hier erst in zweiter Linie, wobei diese Aussage gerade für den Datenschutz beim Glücksspiel gilt. Zunächst geht es in dem Kommentar um den neuen Glücksspiel-Staatsvertrag, der bundesweit einheitliche Regelungen auch zum Online-Glücksspiel enthält. Darin ist vorgesehen, dass Online-Glückspieler sich persönlich registrieren lassen müssen, dass sie während ihres Spiels umfassend überwacht werden, so dass sie keine parallelen Spiele durchführen können, dass Höchsteinsätze gelten und deren Einhaltung überwacht wird. Süchtige Spieler können digital gesperrt werden. Das alles hat zu einer nur unter wenigen Fachleuten geführten Diskussion geführt, ob das nicht ein Zuviel an Überwachung ist. Das Anliegen dieser Regelungen ist zweifellos zu begrüßen: Es geht um die Bekämpfung der Spielsucht, um die Verhinderung glücksspielbedingter Totalverschuldung, um Jugendschutz. Es geht um die Verhinderung illegalen Glücksspiels und der damit zusammenhängenden Finanztransaktionen. Doch kritische Juristen – einschließlich der Konferenz der Datenschutzaufsichtsbehörden in Deutschland – sind sich einig, dass die gefundenen Regelungen nicht mehr als verhältnismäßig angesehen werden können, dass ein berechtigtes Ziel bei der Internetnutzung mit einem Übermaß an Überwachung zu erreichen versucht wird. Das „Länderübergreifende Glücksspielaufsichtssystem" (LUGAS) würde wohl, wenn es verfassungs- oder europarechtlich angegriffen würde, der Rechtskontrolle nicht standhalten.

Dieses Muster ist weit verbreitet: So versuchen die Regierungen in der Europäischen Union (EU) Internet-Kriminalität mit verfassungswidriger Telekommunikations-Vorratsdatenspeicherung zu bekämpfen, was immer wieder höchstgerichtlich zurückgewiesen wird. Derzeit versucht die EU-Kommission Kinderpornografie im Netz durch eine umfassende Chat-Kontrolle einzudämmen. Während über diese Bestrebungen intensiv öffentlich diskutiert wird, gibt es eine solche Diskussion über Online-Glücksspiel nicht, obwohl auch hier ein Berufungsfall geschaffen wurde, den sicher viele Regulatoren gerne ausweiten würden.

Glücksspiel hat also etwas mit Datenschutz zu tun. Das Interesse von Datenschützern für den Handkommentar zum neu geschaffenen Recht ist also gut begründbar. Beim Studium des Werks tritt dann aber Ernüchterung ein: Dort ist die Diskussion (noch?) nicht angekommen. Das Werk ist juristisch gediegen und gibt einen Überblick über sämtliche Rechtsbereiche des Glücksspiels; es kommentiert nicht nur den neuen Glücksspiel-Staatsvertrag, sondern auch weitere einschlägige Regelungen in der Gewerbeordnung, in der Spielverordnung, im Telemediengesetz, im Strafgesetzbuch, im Jugendschutzgesetz, im Rennwett- und Lotteriegesetz, ja sogar im Baugesetzbuch. Länderspezifische Umsetzungsgesetzgebung wird am Beispiel Nordrhein-Westfalen dargestellt. Doch bleibt die Darstellung deskriptiv; eine kritische Auseinandersetzung mit dem bestehenden Recht ist leider nicht zu erkennen, selbst dort, wo sich die erörterten verfassungs- und europarechtlichen Grundlagen hierzu geradezu aufdrängen. So ist der Handkommentar zwar ein sehr geeignetes Nachschlagewerk, wenn es um Absichten der Gesetzgeber und um Entwicklungen dieses Rechtsgebietes geht. Zugleich lässt sich an den vielen Autorinnen und Autoren erkennen, welche Anwaltsgroßkanzleien sich hier empfehlen wollen. Doch die Konflikte, die sich in der Praxis ergeben können, und Positionsbestimmungen hierzu sind nicht zu finden. Selbst eine Bewertung der noch im Aufbau befindlichen zentralisierten staatlichen Aufsicht im Landesverwaltungsamt Sachsen-Anhalt wird vermisst. Insofern ist das Werk zum Nachschlagen der Regelungen und der dahinterstehenden Intentionen in seiner Aktualität und Umfassendheit fast unverzichtbar. Das kritische Hinterfragen muss man dann aber selbstständig und mit anderen Quellen vornehmen.



Sven Krüger
Die KI-Entscheidung – Künstliche Intelligenz und was wir daraus machen
Springer Fachmedien Wiesbaden GmbH, 2021, 29,99 €, ISBN 978-3-658-34873-1

(ha) Das 619 Seiten umfassende Werk von Sven Krüger ist in neun Kapitel unterteilt, die von der allgemeinen Beschreibung („Der Hype, die Medien und die Angst") über die Anfangsfrage, was Künstliche Intelligenz ist und was nicht, zu der Beschreibung von Chatbots bis zum Thema Verantwortung und zu einem Ausblick in die Zukunft führen. Den Kapiteln ist jeweils eine Zusammenfassung vorangestellt und ein Abschnitt der passenden Literatur angehängt. Dem Autor liegt laut Autorenprofil als Berater, Coach und Konzernmanager für Marketing und Digitalisierung die „Vermittlung von Wissen und Fähigkeiten rund um das Thema der digitalen Kompetenz" am Herzen.

Schon auf den ersten Seiten fällt die Marketing-Orientierung der gesamten

Darstellung ins Auge. Auch in der Folge wird Kritik zwar durch zahlreiche Zitate aus Studien und Ausarbeitungen angerissen, aber nicht als Grundeinstellung des Autors erkennbar. So berichtet Krüger beispielsweise völlig euphorisch über Entwicklungen in China: „Kaum anderswo ist sichtbar, was möglich ist, wenn sich eine Gruppe von Menschen konsequent auf ein Thema ausrichtet." In diesem Zusammenhang erwähnt er auch, dass dort „Grundrechte, soweit vorhanden, manipuliert" werden, doch das hindert ihn dann nicht ein Loblied auf schnelle Entwicklung marktfähiger Produkte anzustimmen. Nur nebenbei wird im Zusammenhang mit dem chinesischen Digital Mindset dann erwähnt, dass „KI auf dieser Ebene Raketen steuern, Bewegungen von Bürgern über Kameras verfolgen, Internetzensur erleichtern und Verbrechen vorhersagen" soll.

Da diese umfangreiche Betrachtung des Buchs als eBook vorlag, war ein Durchsuchen nach Stichworten möglich. Dabei stellte sich heraus, dass der Datenschutz schon früh (allerdings eher nebenbei) erwähnt wird. Die Verschlüsselung von Daten findet erst im Zusammenhang mit einem Google-Projekt Erwähnung: „... zwei neuronalen Netzwerken beigebracht haben, wie sie untereinander gesendete Nachrichten verschlüsseln können". Der Autor hält diese Verschlüsselung für sinnvoll, denn „es gibt viele Informationen, die schützenswert sind. Das können industrielle Daten zu Produktionsprozessen sein oder auch einfach Adress- oder Kreditkartendaten einer Online-Bestellung." Auch hier wird wieder die vorrangige Orientierung auf die Interessen der Wirtschaft deutlich.

Bei seinem – vom Rezensenten als wild wahrgenommenen – Durchmarsch durch viele unterschiedliche Anwendungsgebiete von KI stellt der Autor zwar häufiger fest, dass der Datenschutz einerseits eingehalten werden müsse, aber andererseits auch gemäß des Privatsphäre-Paradoxons von den meisten Menschen „als lästig empfunden" werde. Irgendwann aber wertet er die nach der DSGVO geforderte Aufklärung durch Informationstexte ab, indem er konstatiert: „Die meisten sind vernünftig genug nicht ihre kostbare, unwiederbringliche Lebenszeit mit so etwas [dem Lesen] zu verschwenden". Und in einem anderen Kapitel sieht er sich sogar veranlasst das „Berufsbild des Datenschutzbeauftragten" als „in puncto Beliebtheit vergleichbar mit Drückerkolonnen für Rundfunkgebühren" zu bezeichnen. Vielleicht möchte der Autor mit solchen Formulierungen eines seiner im Vorwort ankündigten Ziele erreichen: Das Buch „soll zum Denken anregen". Das tut es sicherlich, wenn auch nicht unbedingt im intendierten Sinn.

Insgesamt liegt eine sehr umfangreiche Sammlung vieler verschiedener KI-Einsatzszenarien vor, die aber allzu oft eine Orientierung auf die Interessen von Datenschutzinteressierten vermissen lässt.



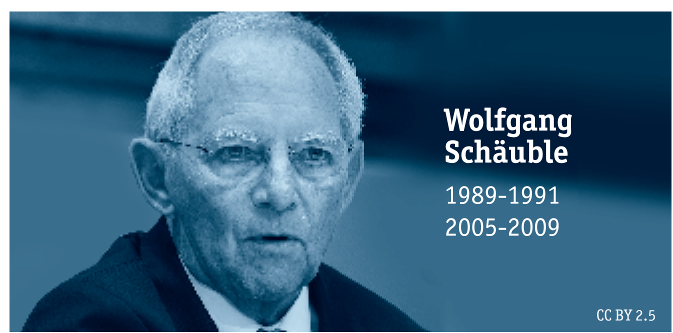
Cartoon

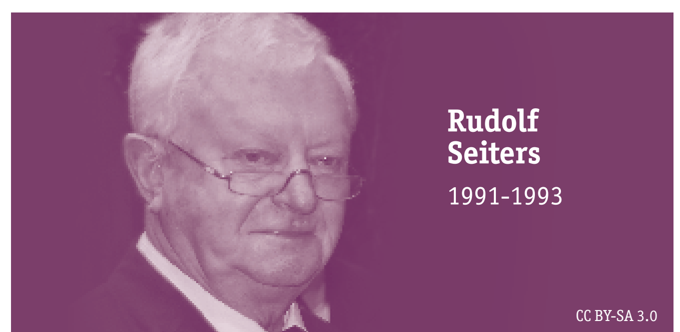




Ein deutscher Innenminister *) setzt sich nach 1982 ernsthaft für Datenschutz und andere Grundrechte ein.





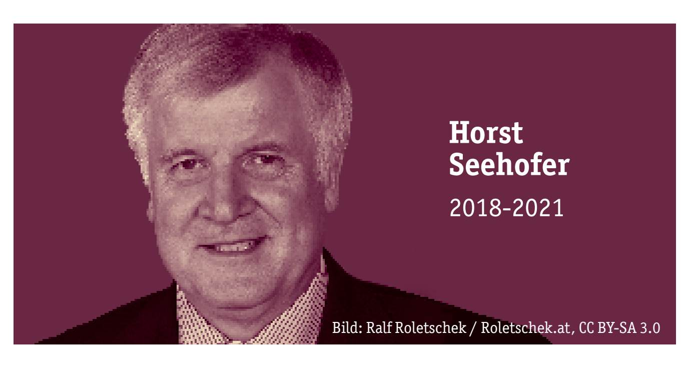












*) Dieser Witz ist bereits vollständig gegendert.